Micronet
Faster and Easier Networks

User's Manual

802.11N Wireless Broadband Router

Model No.: SP916N

http://www.micronet.info

Table of Contents

Chapter 1 Introduction 1
1.1 Package Contents 1
1.2 Key Features 1
1.3 Safety Information 2
1.4 System Requirements 3
1.5 Specifications 3
Chapter 2 Physical Description 4
2.1 Back Panel 4
2.2 Front Panel 4
Chapter 3 System and Network Setup 6
3.1 Build Network Connection 6
3.2 Connecting to Web-Based Management 7
3.2.1 IP Address Configuration 7
3.2.2 Router's IP Address 12
3.2.3 Starting Web-Based Management UI 13
Chapter 4 Web-Based Management UI 15
4.1 Quick Setup Wizard 15
4.2 General Setup 23
4.2.1 System 23
4.2.2 WAN 26
4.2.3 LAN 29
4.2.4 Wireless 31
4.2.5 QoS 42
4.2.6 NAT 44
4.2.7 Firewall 50
4.3 Status 56
4.3.1 System Information 56
4.3.2 Internet Connection Status 57
4.3.3 Device Status 57

4.3.4 System Log 58
4.3.5 Security Log 59
4.3.6 Active DHCP Client 59
4.3.7 Statistics 61
4.4 Configuration Backup and Restore 61
4.5 Firmware Upgrade 62
4.6 System Reset 63
Chapter 5 Glossary 64

Chapter 1 Introduction

Micronet SP916N, 11n Wireless Broadband Router, delivers next generation wireless solution of high speed and cost-efficient network. It is compliant with IEEE 802.11 Draft-N and backward compatible with IEEE 802.11b/g. Best selection for small office where all computers and network devices can share Internet access through a single xDSL/cable modem. In addition, the scope of the network can be easily expanded by connecting the router to a hub or switch.

1.1 Package Contents

Prior to the installation of the device, please verify the following items are in the package:

- SP916N Wireless Broadband Router
- Quick Installation Guide
- Manual CD
- Power Adapter

1.2 Key Features

- High Internet Access throughput (Up to 300Mbps)
- Allow multiple users to share a single Internet line
- Supports up to 253 users
- Share a single Cable or xDSL Internet connection
- Access private LAN servers from the internet
- Four wired LAN ports (10/100M) and one WAN port (10/100M)
- Provides IEEE 802.11b/g/Draft-N wireless LAN capability
- Support DHCP (Server/Client) for easy IP-address setup
- Advanced network and security features like: Special Applications, DMZ, Virtual Servers, Access Control, Firewall.
- Allow you to monitor the router's status like: DHCP Client Log, System Log, Security Log and Device/Connection Status

- Easy to use Web-based GUI for network configuration and management purposes
- Remote management function allows configuration and upgrades from a remote computer (over the Internet)
- Auto MDI / MDI-X function for all wired Ethernet ports.

1.3 Safety Information

In order to keep the safety of users, please follow the following safety instructions:

- This router is designed for indoor use only.
- Do not put this router at or near hot or humid places. Also, do not leave this router in the car in summer.
- Do not pull any connected cable with force and disconnect it from the router first.
- If users want to place this router at high places, please make sure the router is firmly secured. Falling from high places would damage the router and its accessories, and in such cases, the warranty will be void.
- Accessories of this router, like antenna and power supply, are danger to small children under 3 years old. They may put the small parts in their nose or month and it could cause serious damage to them.
- The router will become hot when being used for long time (This is normal and is not a malfunction). Do not put this router on paper, cloth or other flammable materials.
- There’s no user-serviceable part inside the router. If users found the router is not working properly, please contact the authorized dealer of purchase. Do not disassemble the router, otherwise warranty will be void.
- If the router falls into water when it’s powered on, do not use hands to pick it up. Switch the electrical power off before doing anything, or contact an experienced technician for help.
- If users smell something strange, or even see some smoke coming out from the router or power supply, remove the power supply or switch the electrical power off immediately, and call authorized for help.

1.4 System Requirements

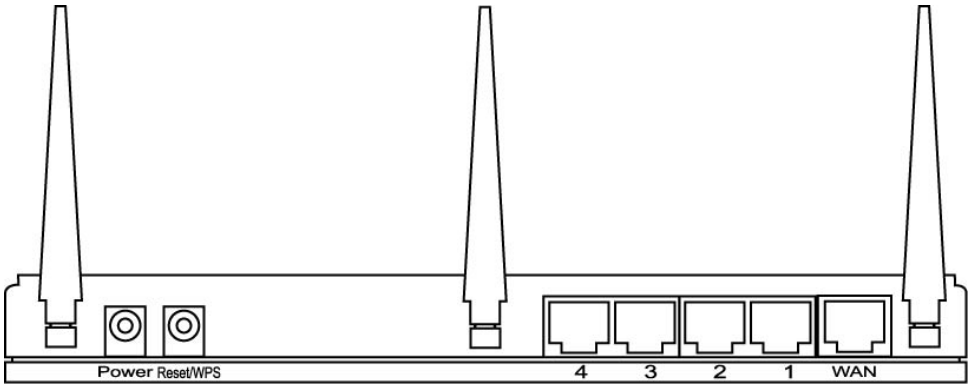
- Internet connection provided by xDSL or cable modem with a RJ-45 Ethernet port.
- Computer or network devices with wired or wireless network interface card.
- Web browsers (Microsoft Internet Explorer 4.0 or above, Netscape Navigator 4.7 or above, Opera web browser or Safari web browser).
- AC power socket (100 – 240V, 50/60Hz).

1.5 Specifications

Standards	IEEE802.11b/ 802.11g / 802.11 Draft-N
Memory	• Flash: 4MB • SDRAM: 16MB
Interface	• WAN Port: 1 x Port 10/100Mbps UTP • LAN Ports: 4 x Port 10/100Mbps UTP
Antenna	3 x Fixed Antenna
MIMO Technology	2T3R MIMO Technology
Transmit Power	16dBm ± 2dBm
DHCP	DHCP Server & Client
Advance Features	• DMZ • Virtual Servers • Access Control • Auto MDI/MDI-X for wired Ethernet ports • Supports QoS (WMM, WMM-PS and WMM-SA)
Security Features	• WEP (64/128 bit) • WPA, WPA2 and WPA Radius • Access Control List (MAC Addresses) • Firewall
Status Log	• DHCP Client Log • System Log • Security Log • Device/Connection Status
Management	• Web-based Interface
Power	12V DC, 1A Power Adapter
Humidity	10-90% (Non-Condensing)
Temperature	32~104 °F (0 ~ 40°C)
Dimension	37 x 194 x 124 mm

Chapter 2 Physical Description

2.1 Back Panel



Parameter	Description
LAN	The Broadband router's 4 LAN ports are where users can connect LAN's PCs, printer servers, hubs and switches etc.
WAN	The WAN port is the segment connected to user's xDSL or Cable modem and is linked to the Internet.
Reset	Press and hold **<Reset/WPS>** button for 20 seconds to clear all settings, and press the button for less than 20 seconds to start WPS function.

2.2 Front Panel

LED	Light Status	Description
PWR	ON	Router's power supply is on
WAN 10/100M	ON	WAN port 100Mbps is connected
	OFF	WAN port 10Mbps is connected

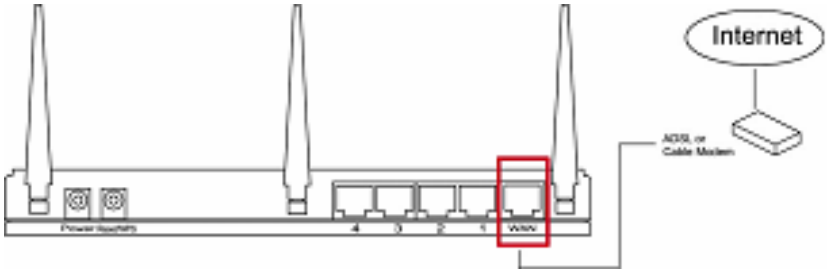
WAN LNK/ACT	ON	WAN is connected
	OFF	No WAN connection
	Flashing	WAN port has Activity (ACT) and data is being sent
LAN 10/100M (Port 1-4)	ON	LAN port speed is 100Mbps
	OFF	LAN port speed is 10Mbps
LAN LNK/ACT (Port 1-4)	ON	LAN is connected
	OFF	No LAN connection
	Flashing	LAN port has Activity (ACT) and data is being sent
WLAN	ON	Wireless LAN or WPS has been activated
	OFF	Wireless LAN is disabled
	Flashing	Wireless LAN port has Activity (ACT) and data is being sent

Chapter 3 System and Network Setup

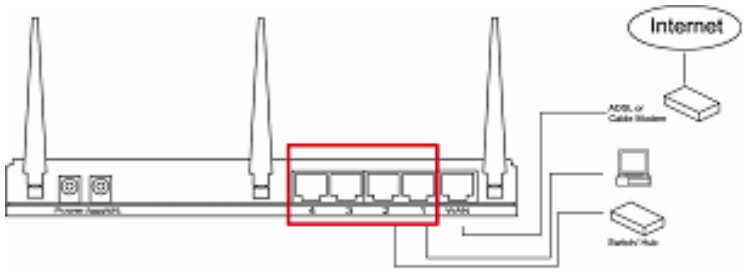
3.1 Build Network Connection

Please follow the following instruction to build the network connection between the new wireless router and other network computers and devices:

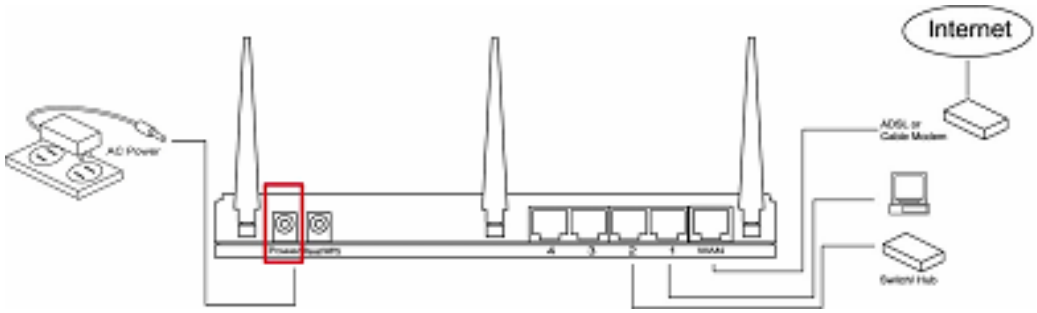
1. Connect the xDSL / cable modem to the WAN port of router by Ethernet cable.



2. Connect all computers, network devices (network-enabled consumer devices other than computers, like game console, or switch / hub) to the LAN port of the router.



3. Connect the power adapter to the wall socket, and then connect it to the ‘Power’ socket of the router.



4. Please check all LEDs on the front panel. ‘PWR’ LED should be steadily on, WAN and LAN LEDs should be on if the computer / network device connected to the respective port of the router is powered on and correctly connected. If PWD LED is not on, or any LED expected is not on, please recheck the cabling, or jump to ‘4-2 Troubleshooting’ for possible reasons and solution.

3.2 Connecting to Web-Based Management

After the network connection is established, the next step is to setup the router with proper network parameters for the user’s network environment.

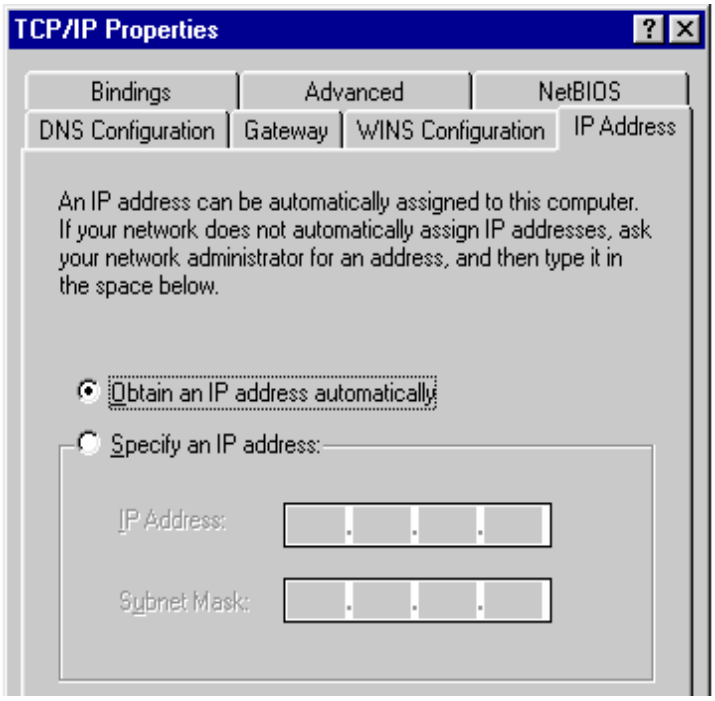
Before connecting to the router and start configuration procedures, user’s computer must be able to get an IP address automatically (use dynamic IP address). If the PC is set to ‘static IP address’, then follow instructions below to reconfigure it to ‘dynamic IP address’.

3.2.1 IP Address Configuration

a) Windows 95/98/Me

1. Click the Start button and select **<Settings>**, then click **<Control Panel>**. The Control Panel window will appear.
2. Double-click on **<Network>** icon. The Network window will appear.
3. Check the list of Network Components. If TCP/IP is not installed, click the **<Add>** button to install it. If TCP/IP is installed, go to step 6.
4. In the Network Component Type dialog box, select **<Protocol>** and click **<Add>** button.
5. In the Select Network Protocol dialog box, select **<Microsoft>** and **<TCP/IP>** then click the **<OK>** button to start installing the TCP/IP protocol. Windows CD may be needed to complete the installation.
6. After installing TCP/IP, go back to the Network dialog box. Select **<TCP/IP>** from the list of Network Components and then click the <Properties> button.
7. Check each of the tabs and verify the following settings:

- Bindings: Check Client for Microsoft Networks and File and printer sharing for Microsoft Networks.
- Gateway: All fields are blank.
- DNS Configuration: Select Disable DNS.
- WINS Configuration: Select Disable WINS Resolution.
- IP Address: Select Obtain IP address automatically.

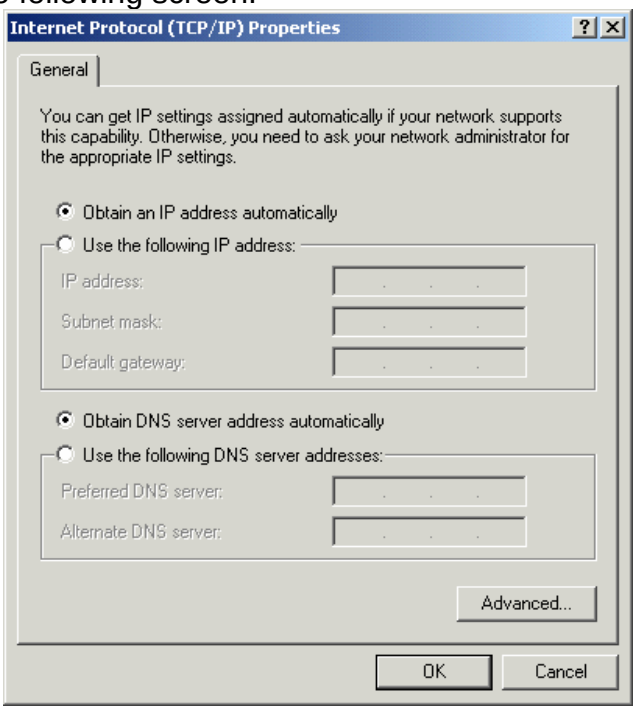

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:

8. Reboot the PC. PC will now obtain an IP address automatically from the Broadband Router's DHCP server.
9. Please make sure that the Broadband router's DHCP server is the only DHCP server available on the LAN network.
10. Proceed to Web-based User Interface once IP address is correctly configured.

b) Windows 2000

1. Click the **<Start>** button and select **<Settings>**, then click **<Control Panel>**. The Control Panel window will appear.
2. Double-click **<Network and Dial-up Connections>** icon. In the Network and Dial-up Connection window, double-click on <Local Area Connection> icon. The Local Area Connection window will appear.
3. In the Local Area Connection window, click the **<Properties>** button.
4. Check the list of Network Components. Users should see Internet Protocol [TCP/IP] on the list. Select it and click the **<Properties>** button.

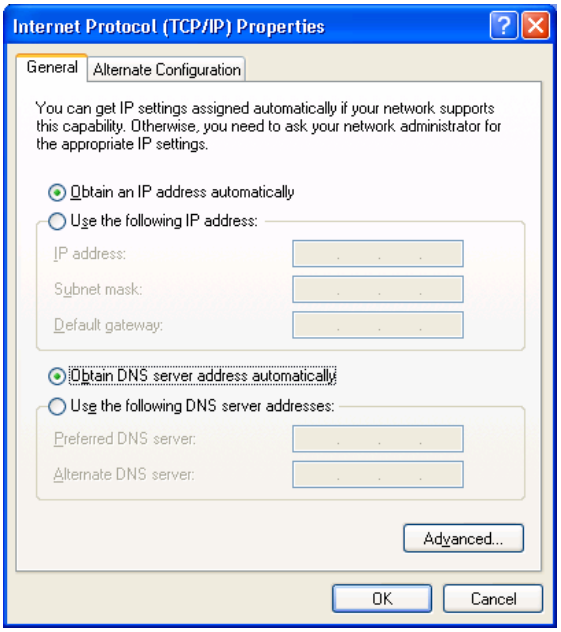
5. In the Internet Protocol (TCP/IP) Properties window, select **<Obtain an IP address automatically>** and **<Obtain DNS server address automatically>** as shown on the following screen.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6. Click **<OK>** to confirm the setting. The PC will now obtain an IP address automatically from the Broadband Router's DHCP server.
7. Please make sure that the Broadband router's DHCP server is the only DHCP server available on the LAN network.
8. Proceed to Web-based User Interface once IP address is correctly configured.

c) Windows XP

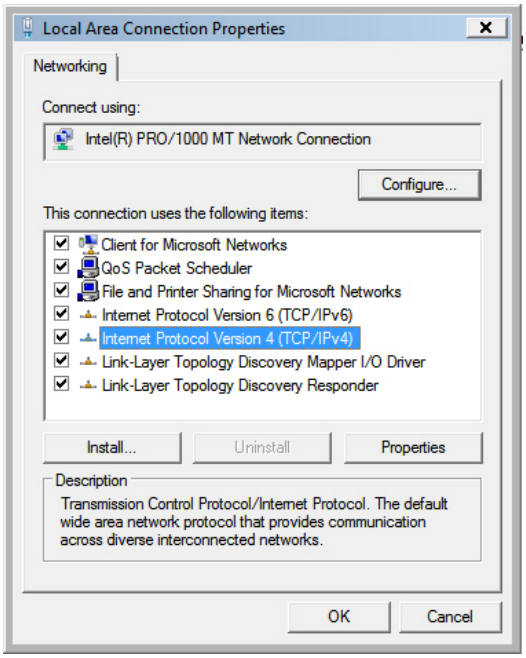
1. Click the **<Start>** button and select **<Settings>**, then click **<Network Connections>**. The Network connections window will appear.
2. Double-click **<Local Area Connection**> icon. The Local Area Connection window will appear.
3. Check the list of Network Components. Users should see Internet Protocol [TCP/IP] on the list. Select it and click the **<Properties>** button.
4. In the Internet Protocol (TCP/IP) Properties window, select **<Obtain an IP address automatically>** and **<Obtain DNS server address automatically>** as shown on the following screen.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

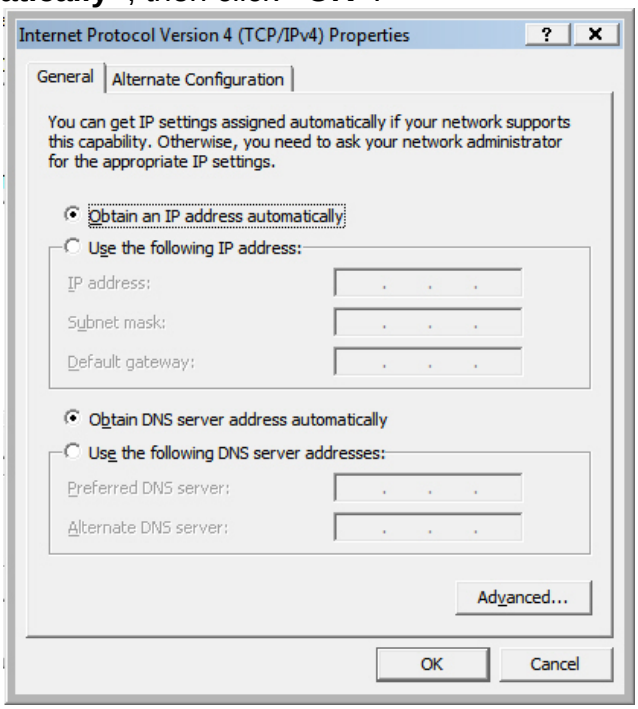
5. Click **<OK>** to confirm the setting. PC will now obtain an IP address automatically from the Broadband Router's DHCP server.
6. Please make sure that the Broadband router's DHCP server is the only DHCP server available on the LAN network.

d) Windows Vista

1. Click **<Start>** button, then click control panel. Click **<View Network Status and Tasks>**, then click **<Manage Network Connections>**. Right-click **<Local Area Network>**, then select **<Properties>**. Local Area Connection Properties window will appear, select **<Internet Protocol Version 4 (TCP / IPv4)>** and click **<Properties>**.



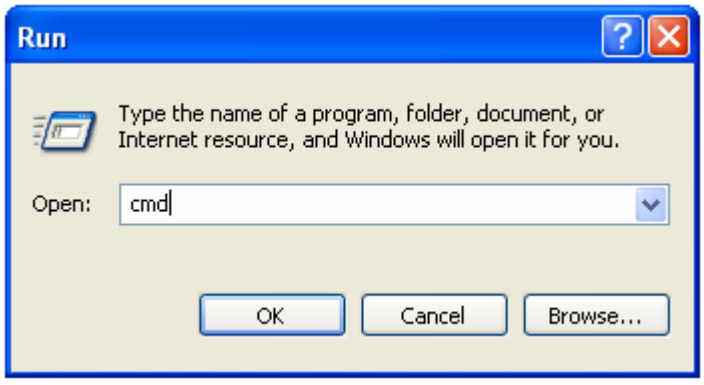
2. Select **<Obtain an IP address automatically>** and **<Obtain DNS server address automatically>**, then click **<OK>**.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

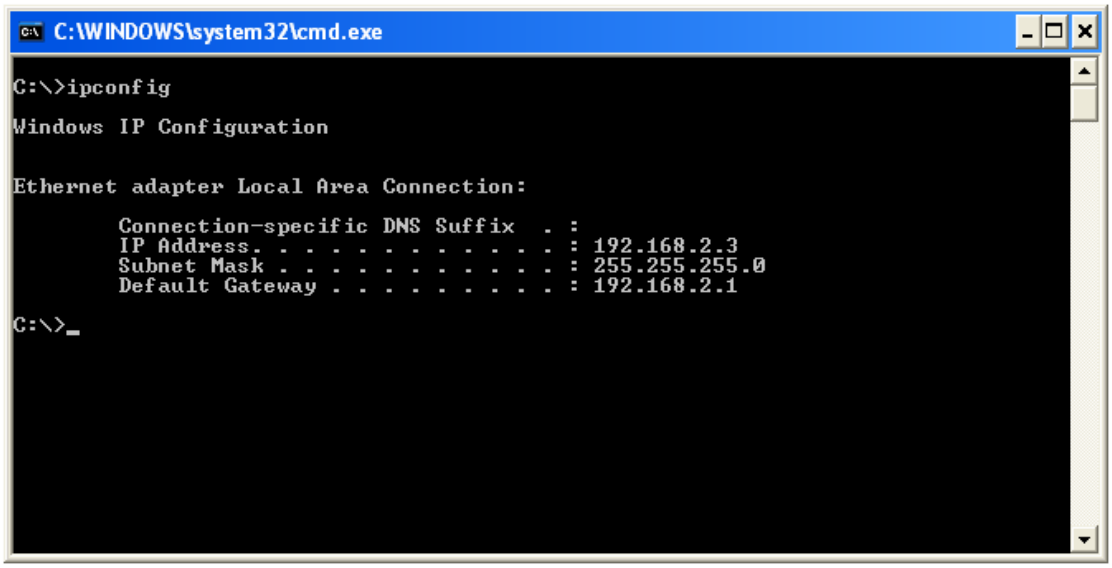
3.2.2 Router's IP Address

1. After the IP address setup is complete, please click **<Start>** then **<Run>** at the bottom lower corner of the desktop.

2. Enter 'cmd' command and click **<OK>**.



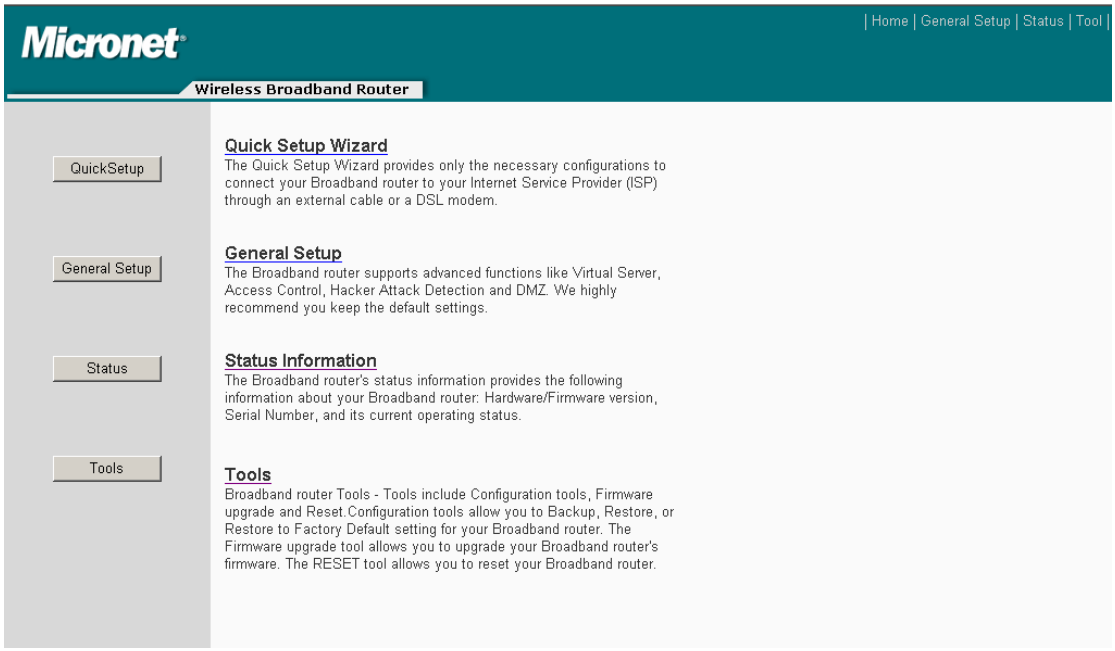
3. Input 'ipconfig', then press 'Enter' key. Please check the IP address followed by 'Default Gateway' (In this example, the IP address of router is 192.168.2.1, please note that this value may be different).


C:\WINDOWS\system32\cmd.exe
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.2.3
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.2.1
C:\>

3.2.3 Starting Web-Based Management UI

1. After the computer has obtained an IP address from router, please start the web browser. Input the IP address of router in the address bar and the following message should appear:

2. Please input username and password in the field respectively. Default username is ‘admin’ and default password is ‘1234’, then press **<OK>** button. Once the login details are entered correctly, users can see the web management interface of this router.


Micronet
Wireless Broadband Router
| Home | General Setup | Status | Tool |
QuickSetup
General Setup
Status
Tools
Quick Setup Wizard
The Quick Setup Wizard provides only the necessary configurations to connect your Broadband router to your Internet Service Provider (ISP) through an external cable or a DSL modem.
General Setup
The Broadband router supports advanced functions like Virtual Server, Access Control, Hacker Attack Detection and DMZ. We highly recommend you keep the default settings.
Status Information
The Broadband router's status information provides the following information about your Broadband router: Hardware/Firmware version, Serial Number, and its current operating status.
Tools
Broadband router Tools - Tools include Configuration tools, Firmware upgrade and Reset.Configuration tools allow you to Backup, Restore, or Restore to Factory Default setting for your Broadband router. The Firmware upgrade tool allows you to upgrade your Broadband router's firmware. The RESET tool allows you to reset your Broadband router.

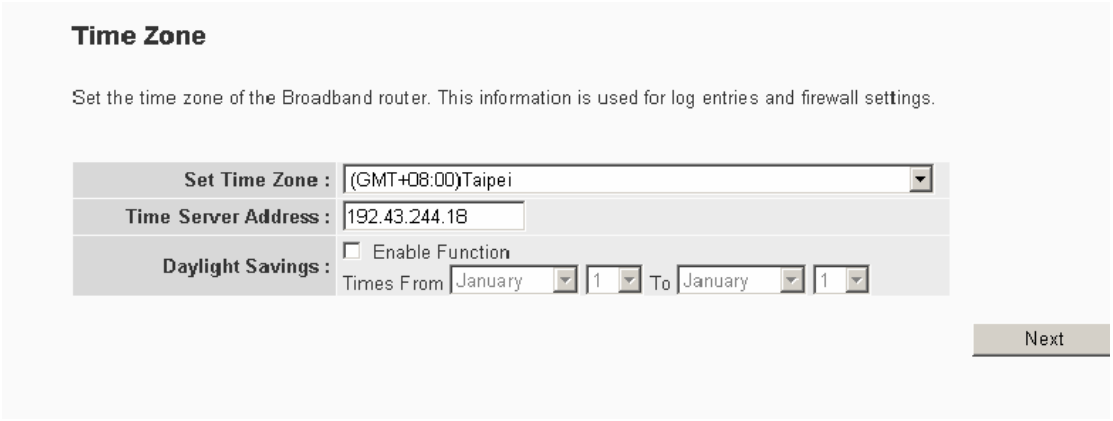
Chapter 4 Web-Based Management UI

4.1 Quick Setup Wizard

The Quick Setup section is designed to get the broadband router running as quickly as possible. In the Quick Setup, users are required to fill in only the information necessary to access the Internet. Once user clicks on the **<Quick Setup Wizard>** in the HOME page, the following screen will appear.

Step 1: Time Zone

The Time Zone allows router to base its time on the settings configured in this section.

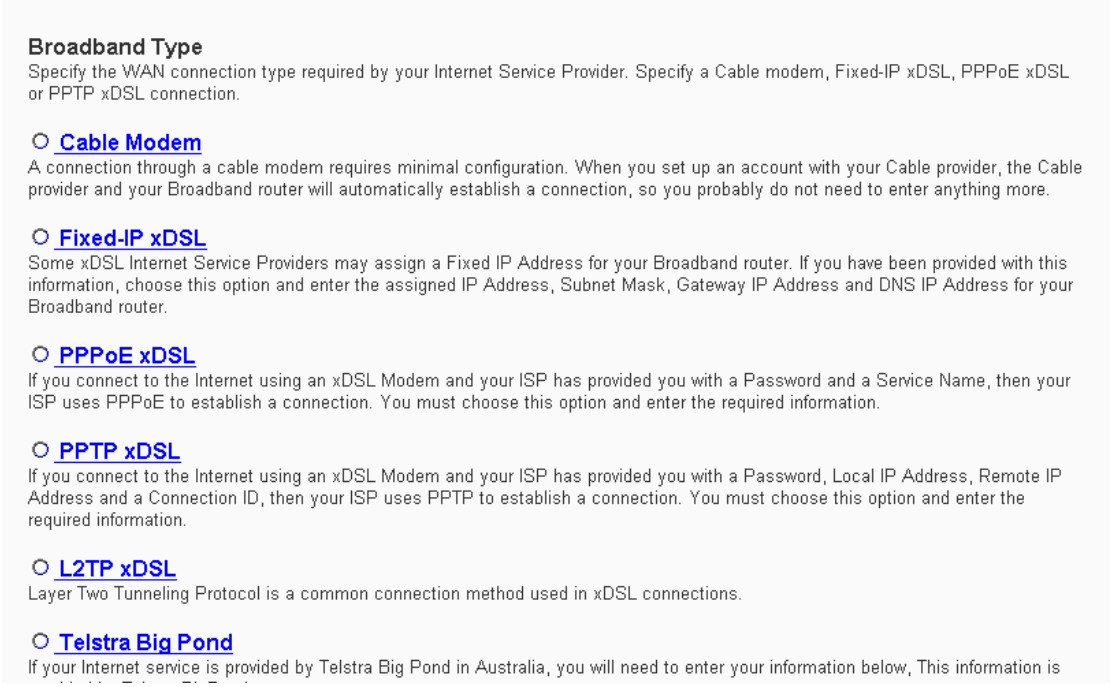

Time Zone
Set the time zone of the Broadband router. This information is used for log entries and firewall settings.
Set Time Zone :
(GMT+08:00)Taipei
Time Server Address :
192.43.244.18
Daylight Savings :
Enable Function
Times From January 1 To January 1
Next

Parameter	Description
Set Time Zone	Select the time zone for the country where the user resides. The router will set its time based on user's selection.
Time Server Address	Users can manually assign time server address if the default time server is not functioning.
Enable Daylight Savings	The router can also take Daylight savings into account. If users wish to use this function, tick the enable box to initiate daylight saving configuration.
Start Daylight Savings Time	Select the period in which to start the daylight savings time.
End Daylight Savings Time	Select the period in which to end the daylight savings time.

*Click on **<NEXT>** to proceed to the next page: Broadband Type.*

Step 2 Broadband Type

In this section users have to select one of four types of connections that it will be using to connect to broadband router WAN port to the ISP (see screen below). Different ISPs require different methods of connecting to the Internet, please check with the ISP as to the type of connection it requires.


Broadband Type
Specify the WAN connection type required by your Internet Service Provider. Specify a Cable modem, Fixed-IP xDSL, PPPoE xDSL or PPTP xDSL connection.
Cable Modem
A connection through a cable modem requires minimal configuration. When you set up an account with your Cable provider, the Cable provider and your Broadband router will automatically establish a connection, so you probably do not need to enter anything more.
Fixed-IP xDSL
Some xDSL Internet Service Providers may assign a Fixed IP Address for your Broadband router. If you have been provided with this information, choose this option and enter the assigned IP Address, Subnet Mask, Gateway IP Address and DNS IP Address for your Broadband router.
PPPoE xDSL
If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password and a Service Name, then your ISP uses PPPoE to establish a connection. You must choose this option and enter the required information.
PPTP xDSL
If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password, Local IP Address, Remote IP Address and a Connection ID, then your ISP uses PPTP to establish a connection. You must choose this option and enter the required information.
L2TP xDSL
Layer Two Tunneling Protocol is a common connection method used in xDSL connections.
Telstra Big Pond
If your Internet service is provided by Telstra Big Pond in Australia, you will need to enter your information below, This information is

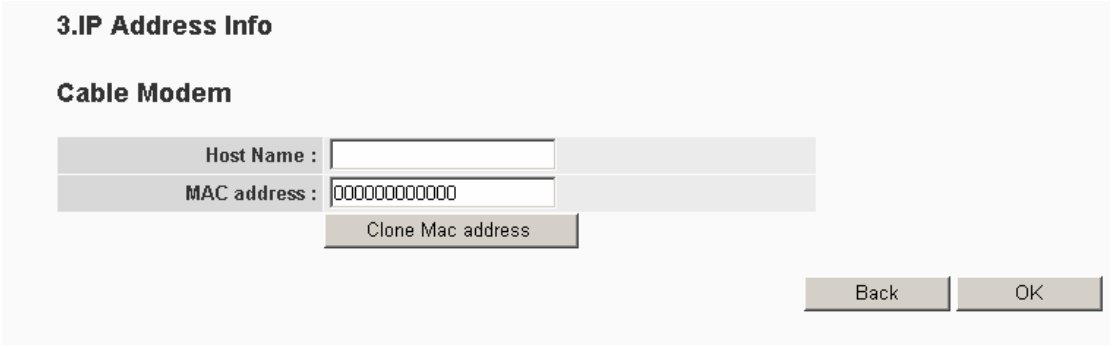
Parameter	Description
Cable Modem	ISP will automatically provide an IP address.
Fixed-IP xDSL	ISP has given users an IP address already.
PPPoE xDSL	ISP requires using a Point-to-Point Protocol over Ethernet (PPPoE) connection.
PPTP xDSL	ISP requires using a Point-to-Point Tunneling Protocol (PPTP) connection.
L2TP xDSL	ISP requires using a Layer Two Tunneling Protocol (L2TP) connection.
Telstra Big Pond	This Protocol only used for Australia's ISP connection.

Click on one of the WAN type and then proceed to the manual's relevant sub-section.

*Click on **<Back>** to return to the previous screen.*

Step 2.1 Cable Modem

Choose Cable Modem if ISP will automatically provide an IP address. Some ISP's may also require users fill in additional information such as Host Name and MAC address (see screen below). The Host Name and MAC address section is optional and users can skip this section if the ISP does not require these settings for Internet connection.

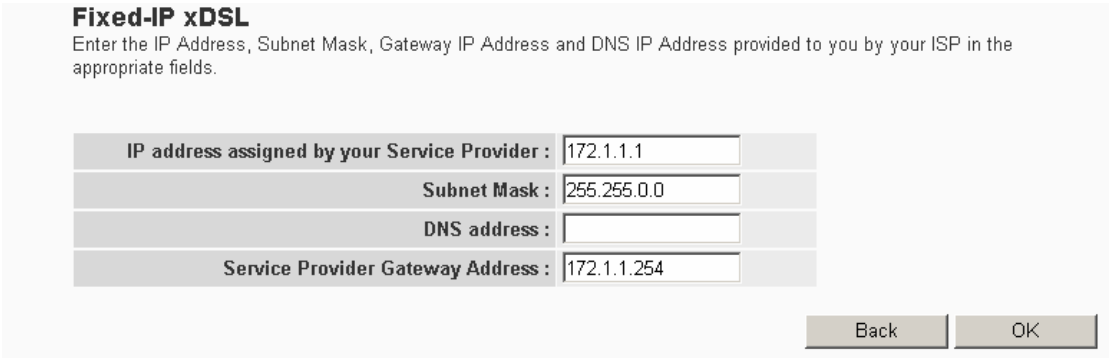


Parameter	Description
Host Name	If the ISP requires a Host Name, type in the host name provided by the ISP, otherwise leave it blank.
MAC Address	ISP may require a particular MAC address in order for users to connect to the Internet. This MAC address is the PC's MAC address that the ISP had originally used to connect to the Internet. Type in this MAC address in this section or use the "Clone MAC Address" button to replace the WAN MAC address with the MAC address of that PC.

*Click **<OK>** to complete the Quick Setup Wizard and start using the broadband router.*

Step 2.2 Fixed-IP xDSL

Select Fixed-IP xDSL if the ISP has given user a specific IP address. The ISP should provide all the information required in this section.

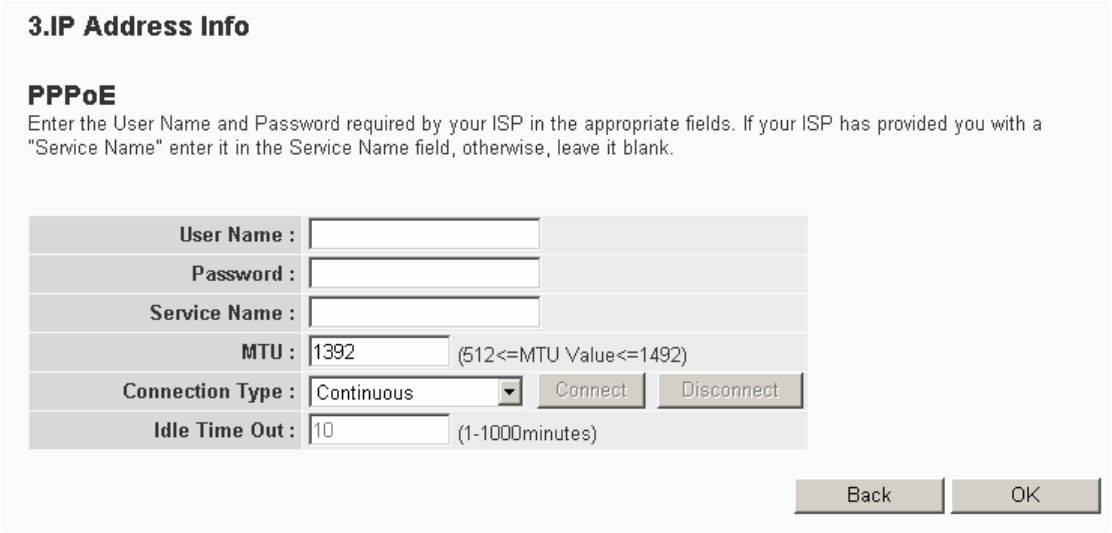

Fixed-IP xDSL
Enter the IP Address, Subnet Mask, Gateway IP Address and DNS IP Address provided to you by your ISP in the appropriate fields.
IP address assigned by your Service Provider :
172.1.1.1
Subnet Mask :
255.255.0.0
DNS address :
Service Provider Gateway Address :
172.1.1.254
Back
OK

Parameter	Description
IP	IP address provided by ISP.
Gateway IP	ISP's IP address gateway.
DNS	ISP's DNS server IP address.
Subnet Mask	Enter the Subnet Mask provided by the ISP (e.g. 255.255.255.0).

*Click **<OK>** to complete the Quick Setup Wizard and start using the broadband router.*

Step 2.3 PPPoE xDSL

Select PPPoE if the ISP requires the PPPoE protocol to connect to the Internet. The ISP should provide all the information required in this section.


3.IP Address Info
PPPoE
Enter the User Name and Password required by your ISP in the appropriate fields. If your ISP has provided you with a "Service Name" enter it in the Service Name field, otherwise, leave it blank.
User Name :
Password :
Service Name :
MTU : 1392 (512<=MTU Value<=1492)
Connection Type : Continuous Connect Disconnect
Idle Time Out : 10 (1-1000minutes)
Back
OK

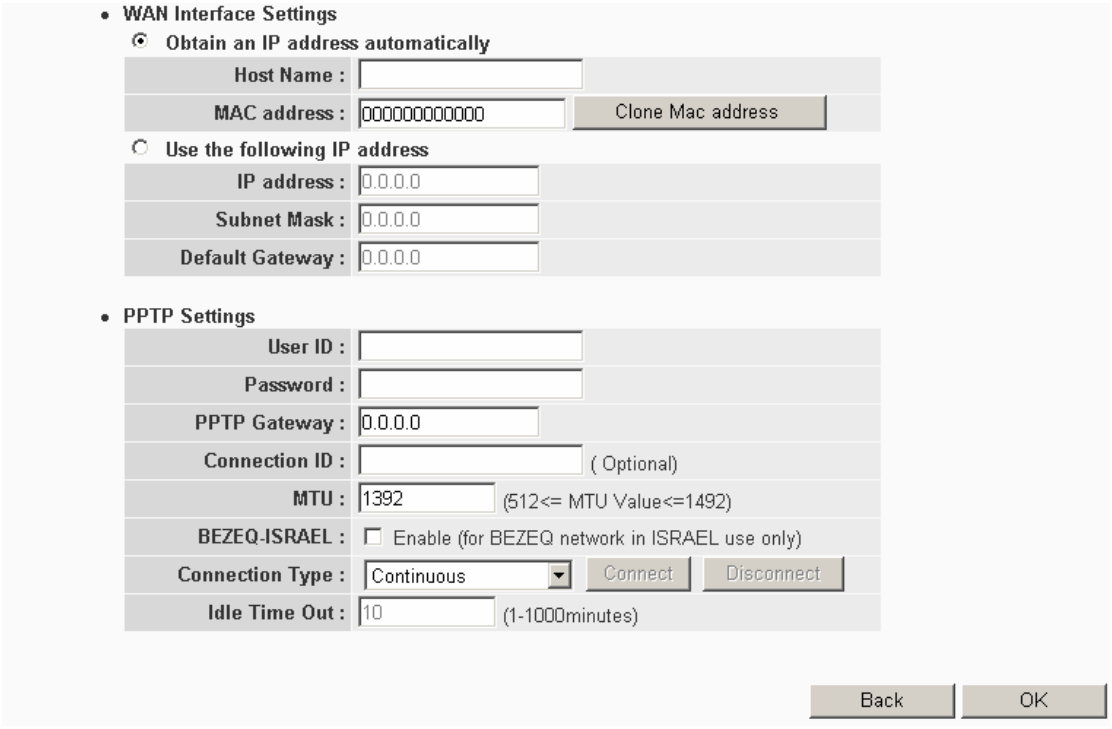
Parameter	Description
Username	Enter the username provided by the ISP for the PPPoE connection.
Password	Enter the password provided by the ISP for the PPPoE connection.
Service Name	This is optional. Enter the Service name should the ISP requires it, otherwise leave it blank.
MTU	This is optional. Users can specify the maximum size of the transmission packet to the Internet. Leave it blank if users do not wish to set a maximum packet size.

Connection Type	• If you select “Continuous”, the router will always connect to the ISP. If the WAN line breaks down and links again, the routers will auto-reconnect to the ISP. • If users select “Connect on Demand”, the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the idle time period exceeds the “Idle Time”. • If users select “Manual”, the router will connect to ISP only when click “Connect” manually from the Web user interface. The WAN connection will not disconnect due to the idle timeout. If the WAN line breaks down and links again, the router will not auto-connect to the ISP.
Idle Time	• Users can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent during the specified period, the router will automatically disconnect the connection with the ISP.

*Click **<OK>** to complete the Quick Setup Wizard and start using the broadband router.*

Step 2.4 PPTP xDSL

Select PPTP if the ISP requires the PPTP protocol to connect to the Internet. The ISP should provide all the information required in this section.

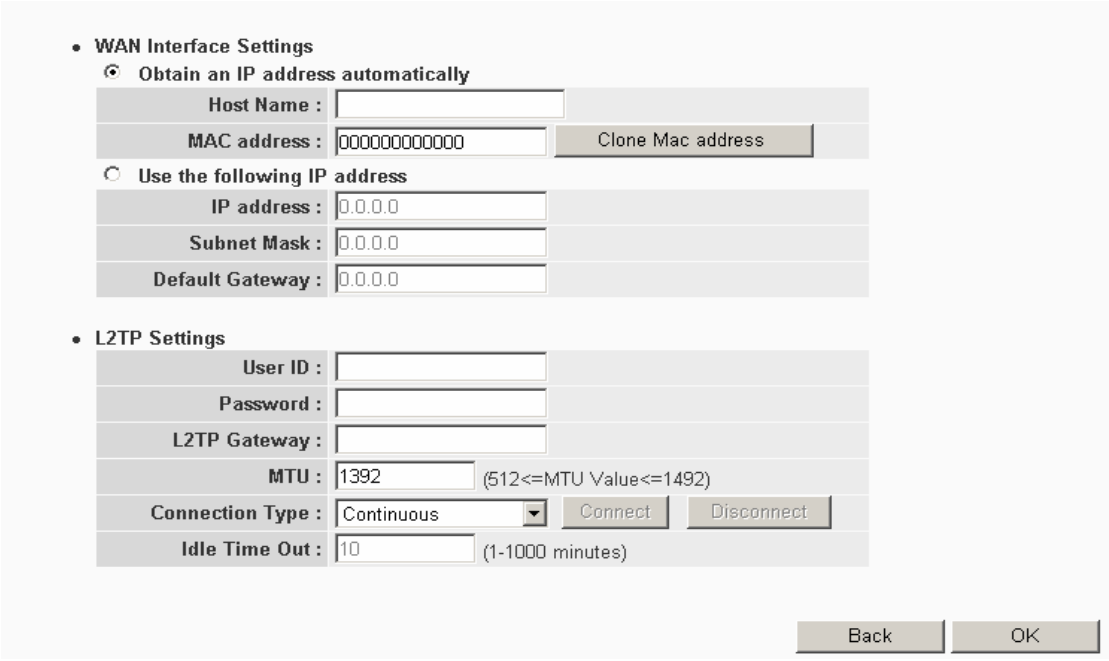


Parameter	Description
Obtain an IP address Automatically	The ISP requires user to obtain an IP address by DHCP before connecting to the PPTP server.
Use the following IP address	The ISP gives user a static IP to be used to connect to the PPTP server.
IP Address	This is the IP address that the ISP has given to user to establish a PPTP connection.
Subnet Mask	Enter the Subnet Mask provided by the ISP (e.g. 255.255.255.0).
Default Gateway	Enter the IP address of the ISP Gateway
User ID	Enter the Username provided by the ISP for the PPTP connection. Sometimes called a Connection ID.
Password	Enter the Password provided by the ISP for the PPTP connection.
PPTP Gateway	If the LAN has a PPTP gateway, then enter that PPTP gateway IP address here. If users do not have a PPTP gateway then enter the ISP's Gateway IP address above.
Connection ID	This is the ID given by ISP. This is optional.
MTU	This is optional. Users can specify the maximum size of the transmission packet to the Internet. Leave it blank if users do not wish to set a maximum packet size.
BEZEQ-ISRAEL	Select this item if users are using the service provided by BEZEQ in Israel.
Connection Type	• If you select "Continuous", the router will always connect to the ISP. If the WAN line breaks down and links again, the routers will auto-reconnect to the ISP. • If users select "Connect on Demand", the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the idle time period exceeds the "Idle Time". • If users select "Manual", the router will connect to ISP only when click "Connect" manually from the Web user interface. The WAN connection will not disconnect due to the idle timeout. If the WAN line breaks down and links again, the router will not auto-connect to the ISP.
Idle Time	• Users can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent during the specified period, the router will automatically disconnect the connection with the ISP. • This "idle timeout" function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet.

*Click **<OK>** to complete the Quick Setup Wizard and start using the broadband router.*

Step 2.5 L2TP

Select L2TP if the ISP requires the L2TP protocol to connect to the Internet. The ISP should provide all the information required in this section.



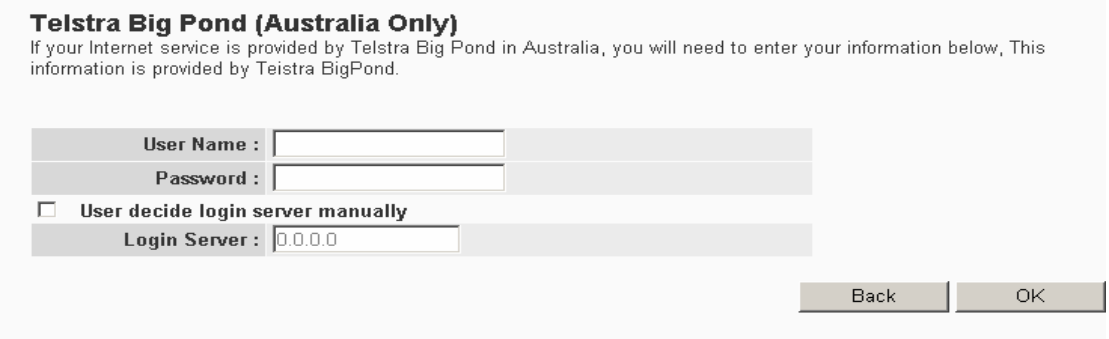
Parameter	Description
Obtain an IP address Automatically	The ISP requires user to obtain an IP address by DHCP before connecting to the L2TP server.
MAC Address	The ISP may require a particular MAC address in order for users to connect to the Internet. Type in this MAC address in this section or use the "Clone MAC Address" button to replace the WAN MAC address with the MAC address of that PC.
Use the following IP address	The ISP gives user a static IP to be used to connect to the L2TP server.
IP Address	This is the IP address that the ISP has given to users to establish a L2TP connection.
Subnet Mask	Enter the Subnet Mask provided by the ISP (e.g. 255.255.255.0).
Gateway	Enter the IP address of the ISP Gateway
User ID	Enter the Username provided by the ISP for the L2TP connection. Sometimes called a Connection ID.
Password	Enter the Password provided by the ISP for the L2TP connection.
L2TP Gateway	If the LAN has a L2TP gateway, then enter that L2TP gateway IP address here. If users do not have a L2TP gateway then enter the ISP's Gateway IP address above.
MTU	This is optional. Users can specify the maximum size of the transmission packet to the Internet. Leave it blank if users do not wish to set a maximum packet size.

Connection Type	• If you select “Continuous”, the router will always connect to the ISP. If the WAN line breaks down and links again, the routers will auto-reconnect to the ISP. • If users select “Connect on Demand”, the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the idle time period exceeds the “Idle Time”. • If users select “Manual”, the router will connect to ISP only when click “Connect” manually from the Web user interface. The WAN connection will not disconnect due to the idle timeout. If the WAN line breaks down and links again, the router will not auto-connect to the ISP.
Idle Time	• Users can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent during the specified period, the router will automatically disconnect the connection with the ISP. • This “idle timeout” function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet.

*Click **<OK>** to complete the Quick Setup Wizard and start using the broadband router.*

Step 2.6 Telstra Big Pond

Select Telstra Big Pond if the ISP requires the Telstra Big Pond protocol to connect to the Internet. The ISP should provide all the information required in this section. Telstra Big Pond protocol is used by the ISP in Australia.

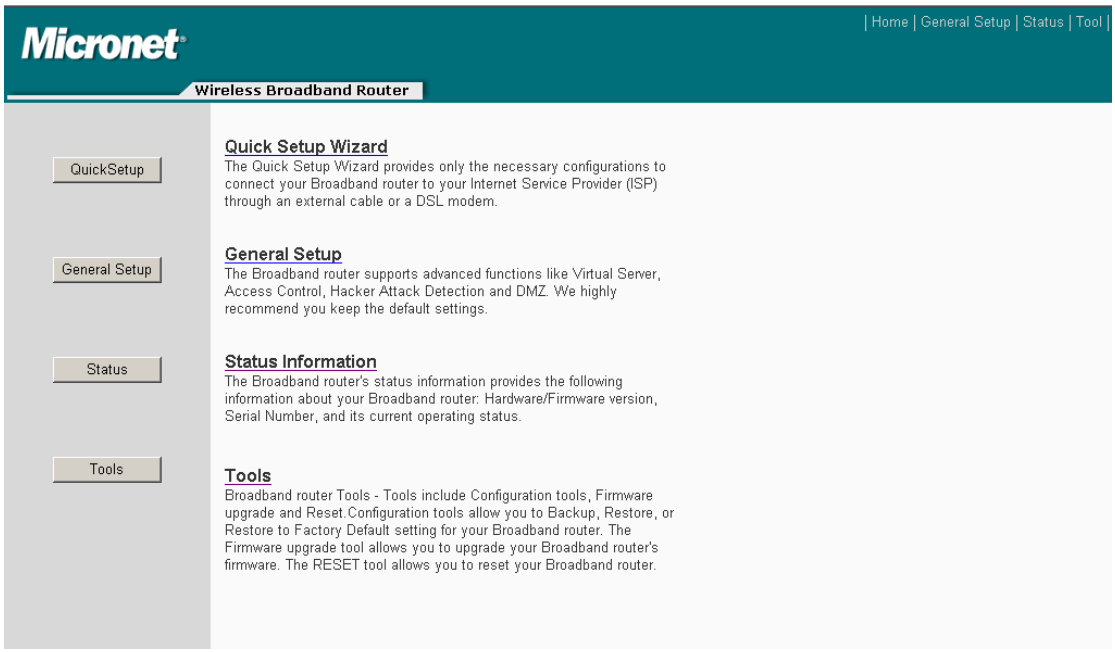

Telstra Big Pond (Australia Only)
If your Internet service is provided by Telstra Big Pond in Australia, you will need to enter your information below, This information is provided by Teistra BigPond.
User Name :
Password :
User decide login server manually
Login Server :
0.0.0.0
Back
OK

Parameter	Description
Username	Enter the username provided by the ISP for the Telstra Big Pond connection.
Password	Enter the password provided by the ISP for the Telstra Big Pond connection.
User Decide Login Server Manually	Select if users want to assign the IP of Telstra Big Pond’s login server manually.
Login Server	The IP address of the login server.

*Click **<OK>** to complete the Quick Setup Wizard and start using the broadband router.*

4.2 General Setup

In this chapter, the user will know how to change the time zone, password, and remote management settings. Please start the web browser and log onto router web management interface, then click ‘General Setup’ button on the left, or click ‘General Setup’ link at the upper-right corner of web management interface.

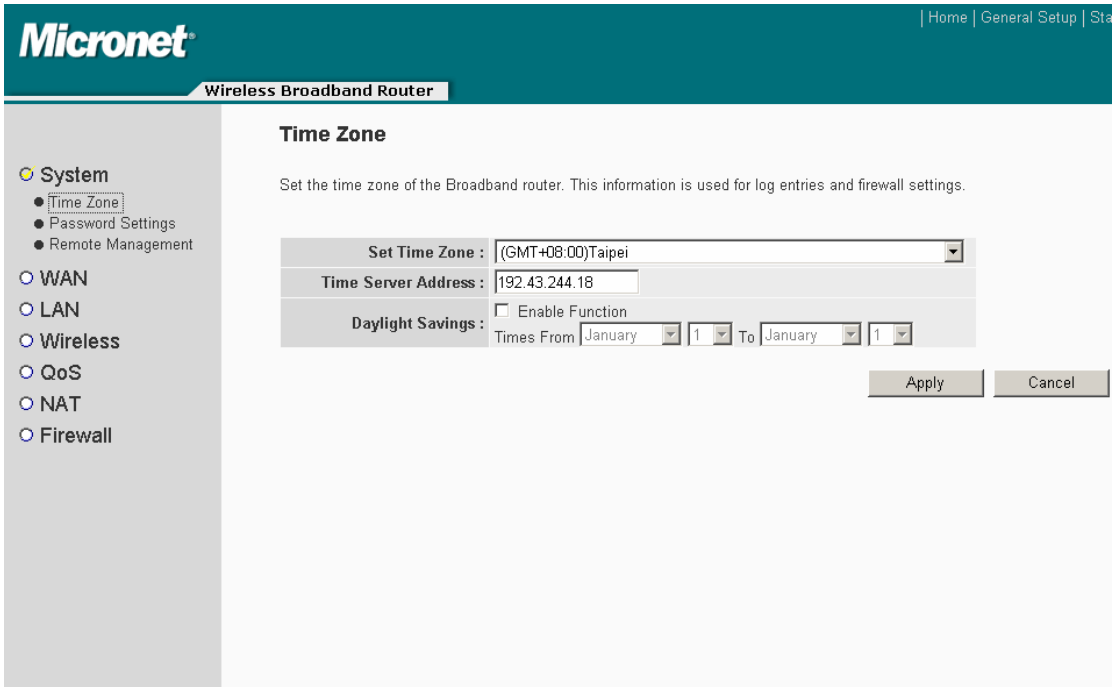

Micronet
Wireless Broadband Router
| Home | General Setup | Status | Tool |
QuickSetup
General Setup
Status
Tools
Quick Setup Wizard
The Quick Setup Wizard provides only the necessary configurations to connect your Broadband router to your Internet Service Provider (ISP) through an external cable or a DSL modem.
General Setup
The Broadband router supports advanced functions like Virtual Server, Access Control, Hacker Attack Detection and DMZ. We highly recommend you keep the default settings.
Status Information
The Broadband router's status information provides the following information about your Broadband router: Hardware/Firmware version, Serial Number, and its current operating status.
Tools
Broadband router Tools - Tools include Configuration tools, Firmware upgrade and Reset.Configuration tools allow you to Backup, Restore, or Restore to Factory Default setting for your Broadband router. The Firmware upgrade tool allows you to upgrade your Broadband router's firmware. The RESET tool allows you to reset your Broadband router.

4.2.1 System

This section allows user to set the following system configuration: Time Zone, Password and Remote Management Administrator.

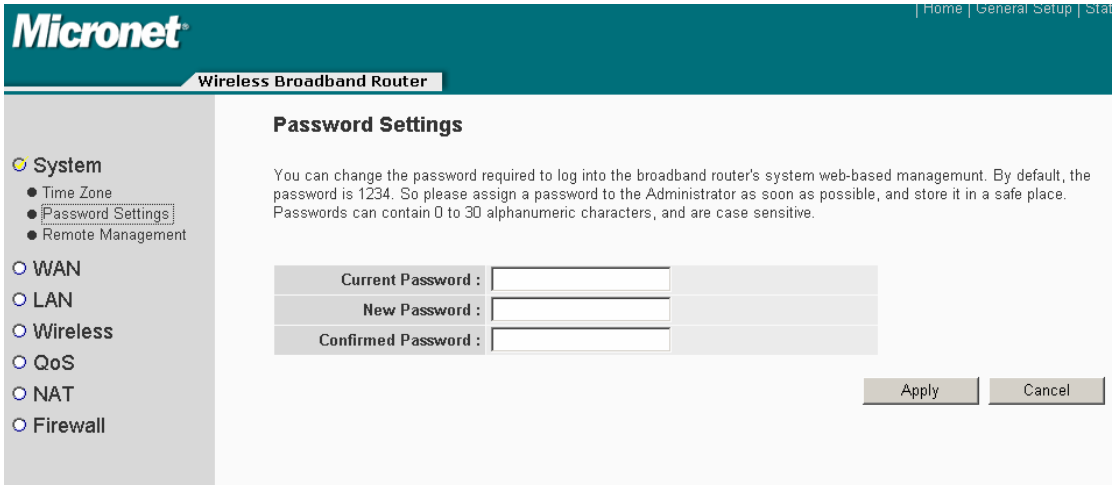
4.2.1.1 Time zone and Time Auto-synchronization

Please click ‘System’ menu on the left of web management interface, then click ‘Time Zone’, and the following message will be displayed on the web browser: Please select time zone at ‘Set time zone’ drop-down list, and input the IP address or host name of time server. If users want to enable daylight savings setting, please check ‘Enable Function’ box, and set the duration of daylight setting.



4.2.1.2 Password Setting

Default password of this router is ‘1234’, and it’s displayed on the login prompt when accessed from web browser. There’s a security risk if users don’t change the default password, since everyone can see it. This is very important when the wireless function is enabled. Please click ‘System’ menu on the left of web management interface, then click ‘Password Settings’. The following message will be displayed on your web browser:

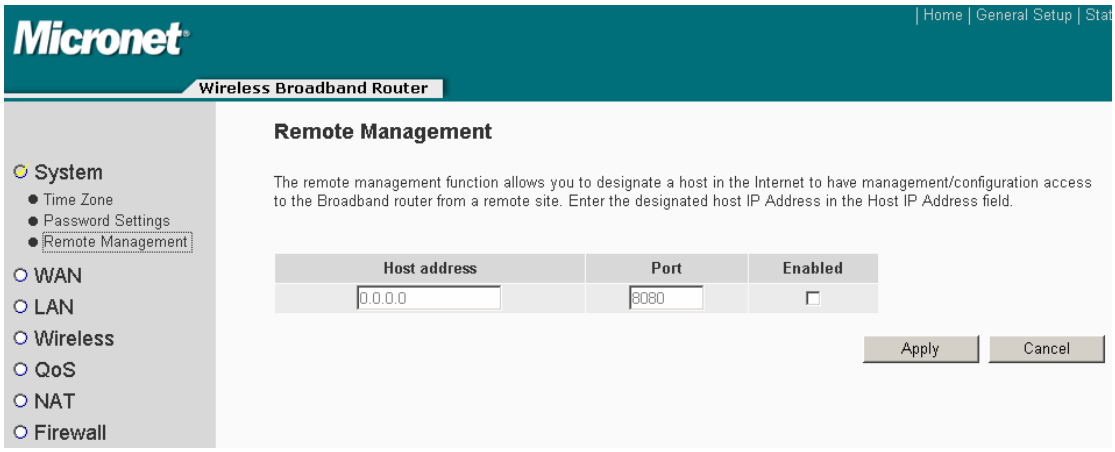

Micronet
Wireless Broadband Router
| Home | General Setup | Stat
System
Time Zone
Password Settings
Remote Management
WAN
LAN
Wireless
QoS
NAT
Firewall
Password Settings
You can change the password required to log into the broadband router's system web-based managemunt. By default, the password is 1234. So please assign a password to the Administrator as soon as possible, and store it in a safe place. Passwords can contain 0 to 30 alphanumeric characters, and are case sensitive.
Current Password :
New Password :
Confirmed Password :
Apply
Cancel

Parameter	Description
Current Password	Enter user's current password for the remote management administrator to login to your Broadband router. *Default: no password*
New Password	Enter the new password.
Confirmed Password	Enter the new password again for verification purposes. If users forget the password, it will be necessary to reset the router to the factory default (No password) with the reset button (see router's back panel).

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

4.2.1.3 Remote Management

This router does not allow management access from Internet, to prevent possible security risks (especially when users defined a weak password, or didn't change default password). However, users can still manage this router from a specific IP address by enabling the 'Remote Management'.

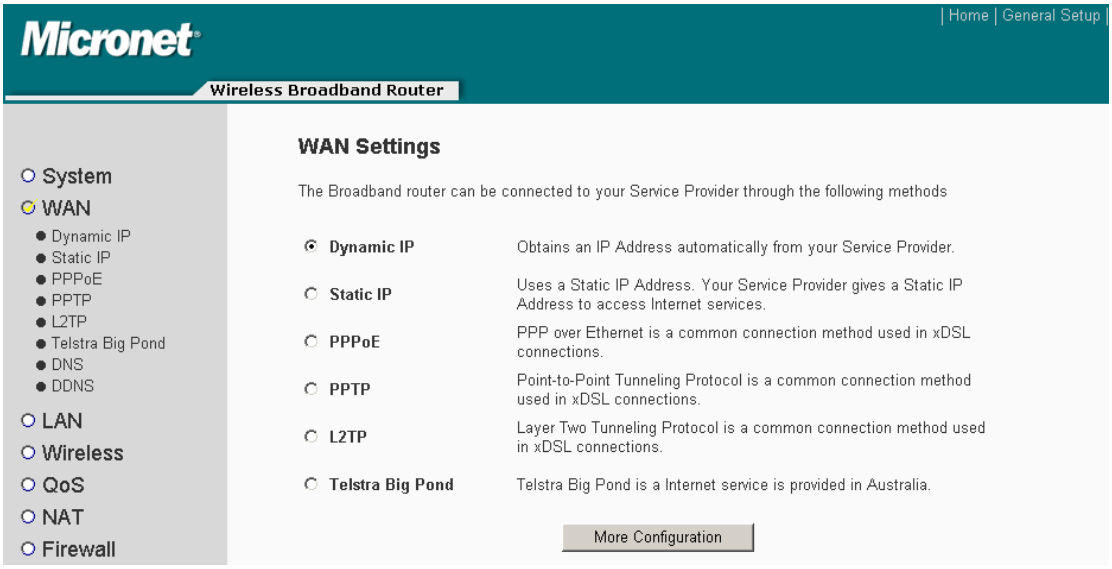


Parameter	Description
Host Address	• This is the IP address of the host in the Internet that will have management/configuration access to the Broadband router from a remote site. This means if users are at home and the home IP address has been designated the Remote Management host IP address for this router (located in your company office), then it will be able to configure this router remotely. • If the Host Address is left 0.0.0.0, it would mean anyone can access the router's web-based configuration from a remote location, provided password is known. • When users want to access the web-based management from a remote site, it is necessary to enter the router's WAN IP address (e.g. 10.0.0.1) into your web-browser followed by port number 8080 (e.g. 10.0.0.1:8080). Users also need to know the password set in the Password Setting screen in order to access the router's web-based management.

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

4.2.2 WAN

Internet connections setup can be setup by using 'Quick Setup' menu described in chapter 4.1. However, users can setup WAN connections up by using WAN configuration menu. Users can also set advanced functions like DDNS (Dynamic DNS) via this interface.

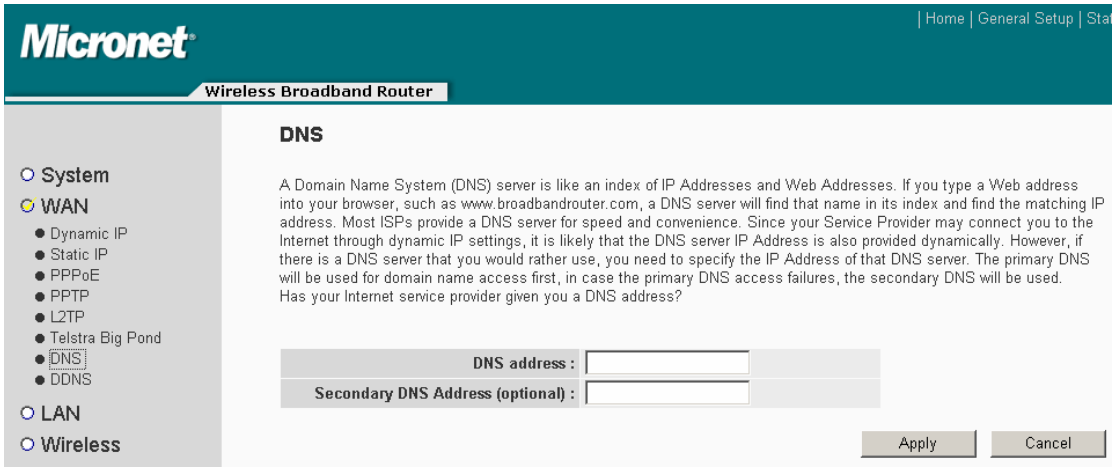

Micronet
Wireless Broadband Router
| Home | General Setup |
System
WAN
Dynamic IP
Static IP
PPPoE
PPTP
L2TP
Telstra Big Pond
DNS
DDNS
LAN
Wireless
QoS
NAT
Firewall
WAN Settings
The Broadband router can be connected to your Service Provider through the following methods
Dynamic IP
Obtains an IP Address automatically from your Service Provider.
Static IP
Uses a Static IP Address. Your Service Provider gives a Static IP Address to access Internet services.
PPPoE
PPP over Ethernet is a common connection method used in xDSL connections.
PPTP
Point-to-Point Tunneling Protocol is a common connection method used in xDSL connections.
L2TP
Layer Two Tunneling Protocol is a common connection method used in xDSL connections.
Telstra Big Pond
Telstra Big Pond is a Internet service is provided in Australia.
More Configuration

Parameter	Description
Dynamic IP address	ISP will automatically give user an IP address. Follow section 4.1 “Cable Modem” for detail information.
Static IP address	ISP has given user an IP address already. Follow section 4.1 “Fixed IP” for detail information.
PPPoE	ISP requires using a Point-to-Point Protocol over Ethernet (PPPoE) connection. Follow section 4.1 “PPPoE” for detail information.
PPTP	ISP requires using a Point-to-Point Tunneling Protocol (PPTP) connection. Follow section 4.1 “PPTP” for detail information.
L2TP	ISP requires using a Layer Two Tunneling Protocol (L2TP) connection.
Telstra Big Pond	This Protocol only used for Australia’s ISP connection. Follow section 4.1 “Telstra Big Pond” for detail information.
DNS	Users can specify a DNS server.
DDNS	Users can specify a DDNS server and configure the username and password provided by the DDNS service provider.

*Click **<More Configuration>** at the bottom of the screen and proceed to the manual’s relevant sub-section.*

4.2.2.1 DNS

A Domain Name System (DNS) server is like an index of IP addresses and Web addresses. If users type a Web address into the browser, such as www.router.com, a DNS server will find that name in its index and the matching IP address. Most ISPs provide a DNS server for speed and convenience. If the Service Provider connects the user to the Internet with dynamic IP settings, it is likely that the DNS server IP address is provided automatically. However, if there is a DNS server that the user would rather use, it is necessary to specify the IP address of that DNS server in this section.

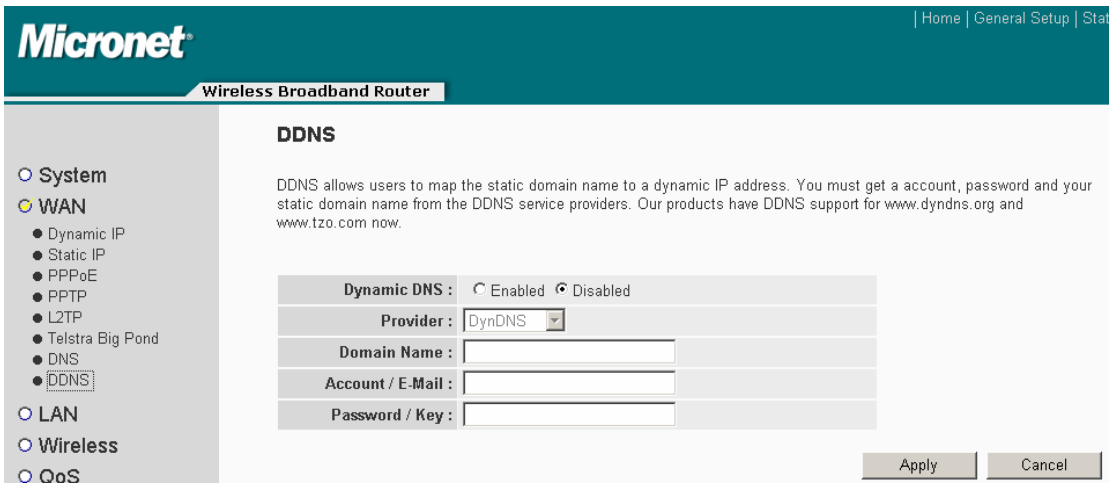

Micronet
Wireless Broadband Router
| Home | General Setup | Stat
System
WAN
Dynamic IP
Static IP
PPPoE
PPTP
L2TP
Telstra Big Pond
DNS
DDNS
LAN
Wireless
DNS
A Domain Name System (DNS) server is like an index of IP Addresses and Web Addresses. If you type a Web address into your browser, such as www.broadbandrouter.com, a DNS server will find that name in its index and find the matching IP address. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect you to the Internet through dynamic IP settings, it is likely that the DNS server IP Address is also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP Address of that DNS server. The primary DNS will be used for domain name access first, in case the primary DNS access failures, the secondary DNS will be used.
Has your Internet service provider given you a DNS address?
DNS address :
Secondary DNS Address (optional) :
Apply
Cancel

Parameter	Description
Domain Name Server (DNS) Server	This is the DNS server IP address provided by ISP. Users can specify preferred DNS server IP address.
Secondary DNS Address (optional)	This is optional. Users can enter another DNS server's IP address as a backup. The secondary DNS will be used should the primary DNS fail.

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

4.2.2.2 DDNS

DDNS allows user to map the static domain name to a dynamic IP address. Users must get an account, password and static domain name from the DDNS service providers. This router supports DynDNS, TZO and other common DDNS service providers.

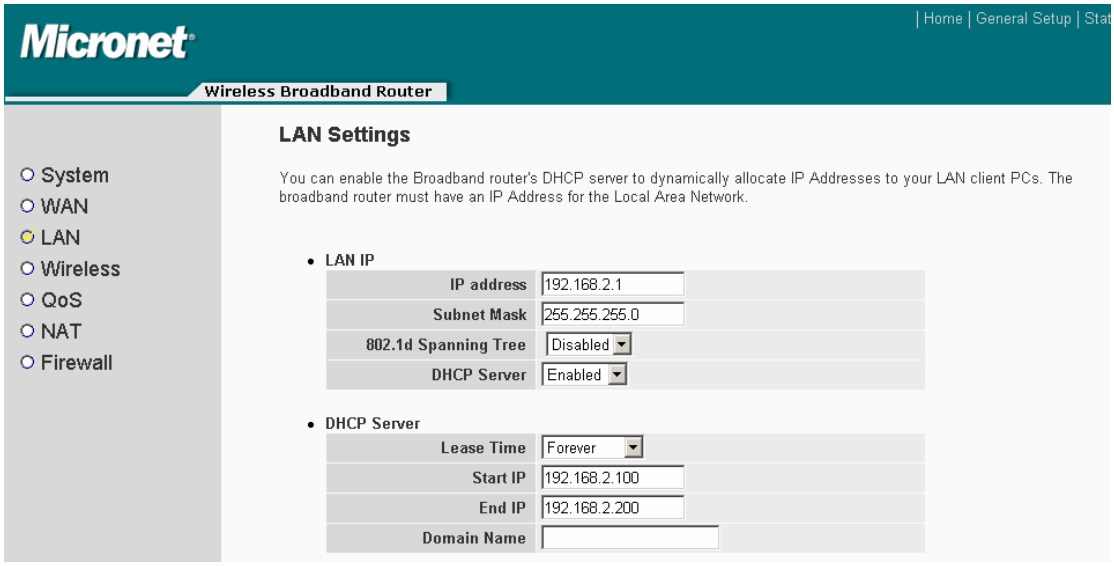


Parameter	Description
Enable/Disable	Enable or Disable the DDNS function of this router.
Provider	Select a DDNS service provider.
Domain name	User's static domain name that use DDNS.
Account/E-mail	The account that the DDNS service provider assigned to user.
Password/Key	The password set for the DDNS service account above.

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

4.2.3 LAN

Before all computers using wired Ethernet connection (i.e. those computers connect to this router's LAN port 1 to 4 by Ethernet cable) can communicate with each other and access internet, they must have a valid IP address. There are two ways to assign IP addresses to computers: static IP address (set the IP address for every computer manually), and dynamic IP address (IP address of computers will be assigned by router automatically). It's recommended for most of computers to use dynamic IP address, since it will save a lot of time on setting IP addresses. DHCP settings are only available when 'DHCP Server' in 'LAN IP' section is 'Enabled'.



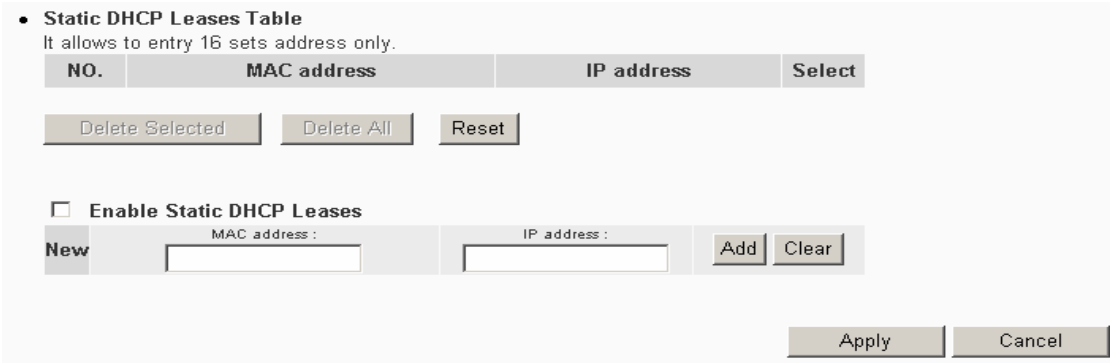
Parameter	Description
IP address	This is the router's LAN port IP address (LAN clients default gateway IP address).
IP Subnet Mask	Specify a Subnet Mask for the LAN segment.

802.1d Spanning Tree	If 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent from network loop happening in the LAN ports.
DHCP Server	Users can enable or disable the DHCP server. By enabling the DHCP server, the router will automatically give LAN clients an IP address. If the DHCP is not enabled then users will have to manually set the LAN client's IP addresses. Make sure the LAN Client is in the same subnet as this broadband router for the router to be the LAN client's default gateway.
Lease Time	The DHCP when enabled will temporarily give the LAN clients an IP address. In the Lease Time setting, users can specify the time period that the DHCP lends an IP address to the LAN clients. The DHCP will change the LAN client's IP address when this time threshold period is reached.
IP Address Pool	Users can select a particular IP address range for the DHCP server to issue IP addresses to LAN Clients.
Domain Name	Users can specify a Domain Name for the LAN network.

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

4.2.3.1 Static DHCP Leases Table

This function allows user to assign a static IP address to a specific computer so that it is not necessary to set the IP address for a computer, and still enjoy the benefit of using DHCP server. Maximum 16 static IP addresses can be assigned here.

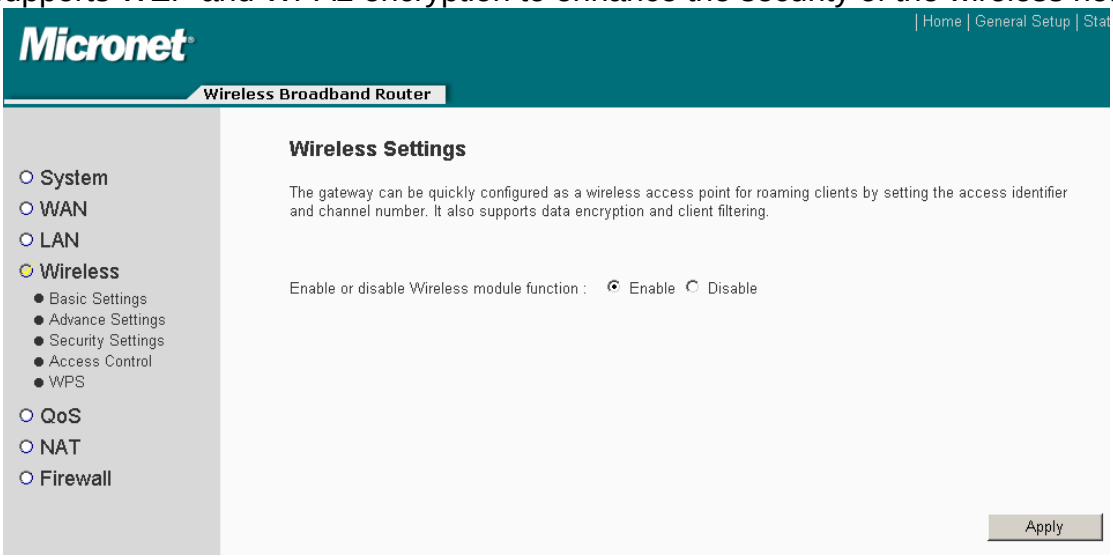


Parameter	Description
Enable Static DHCP Leases	Check this box to enable this function.
MAC Address	Input the MAC address of the computer or network device.
IP address	Input the IP address to assign to this computer or network device.

*Click **<Add>** to enter the entry into the table, otherwise click on **<Clear>** to remove all characters.*

4.2.4 Wireless

Wireless Broadband Router builds a wireless LAN and can let all PCs equipped with IEEE 802.11b or 801.11g wireless network adaptor connect to the Intranet and Internet. It supports WEP and WPA2 encryption to enhance the security of the wireless network.

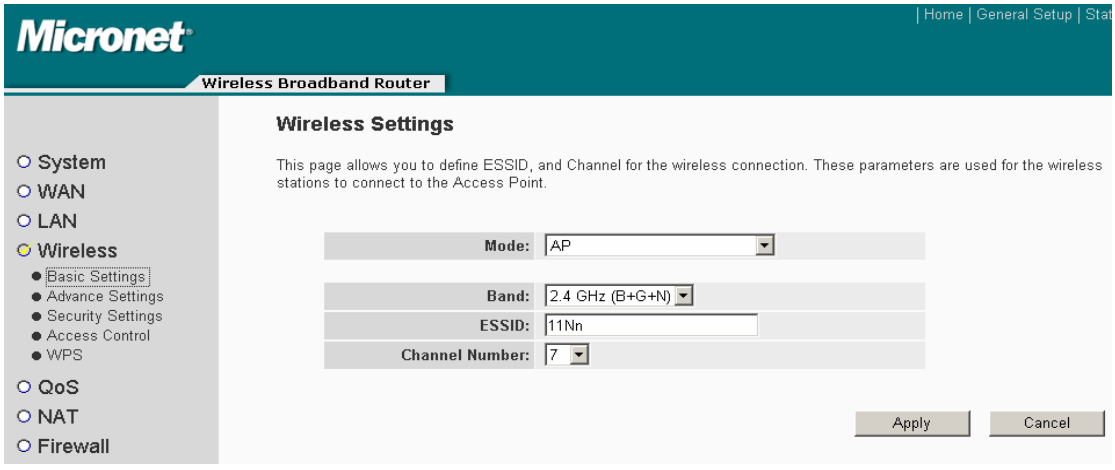


Parameter	Description
Enable or Disable Wireless Module Function	Users can select to enable or disable the wireless connection of this device.

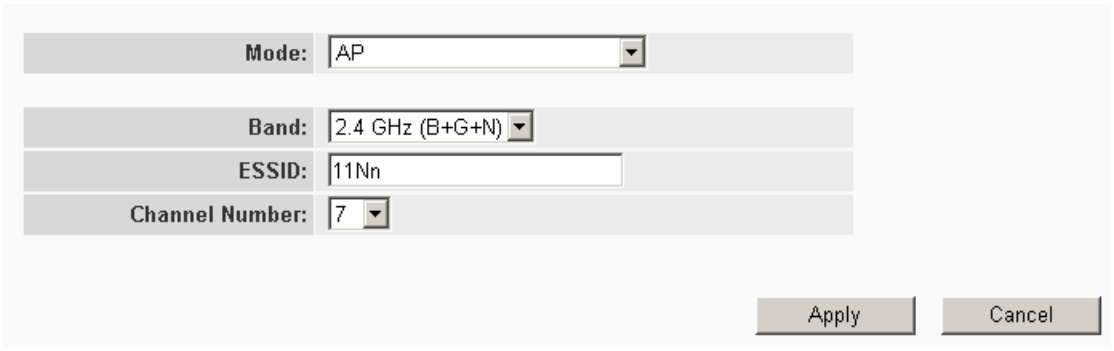
*Click **<Apply>** at the bottom of the screen to save the above configurations.*

4.2.4.1 Basic Wireless Setting

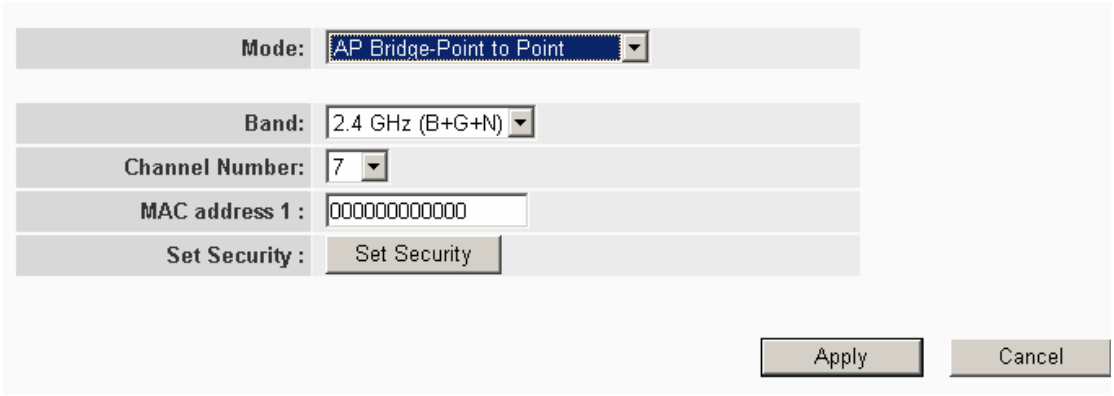
Please click 'Wireless' menu on the left of web management interface, then click 'Basic Settings', and the following message will be displayed on the web browser.



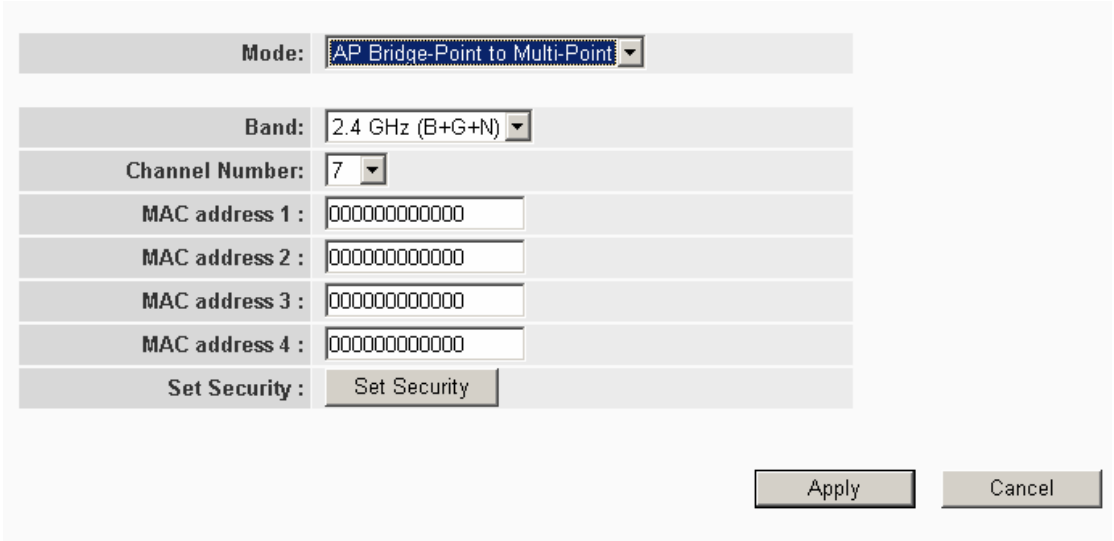
Mode: AP



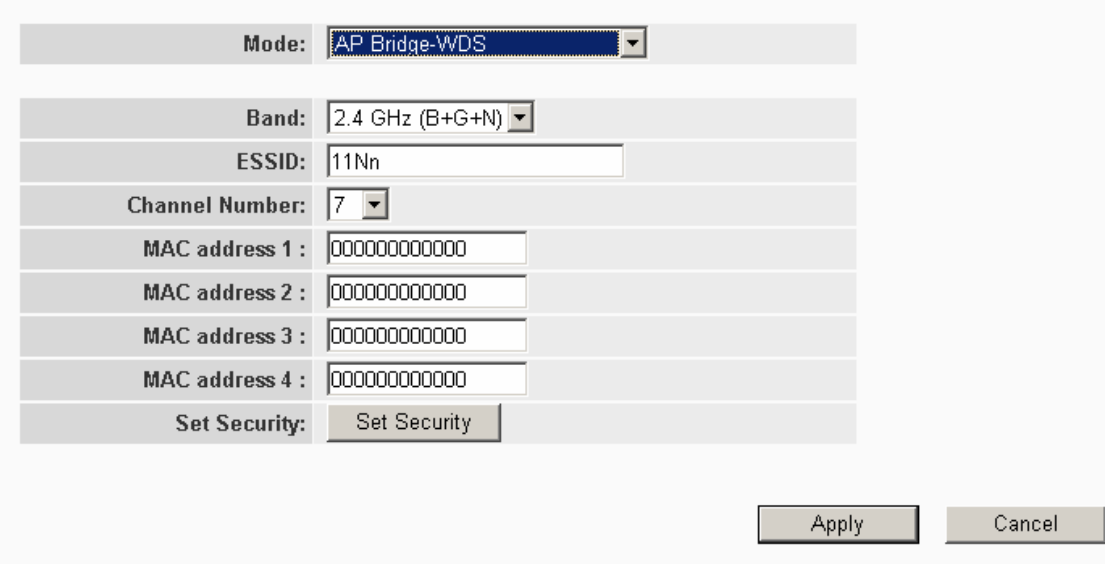
Mode: AP Bridge-Point to Point



Mode: AP Bridge-Point to Multi-Point



Mode: AP Bridge-WDS

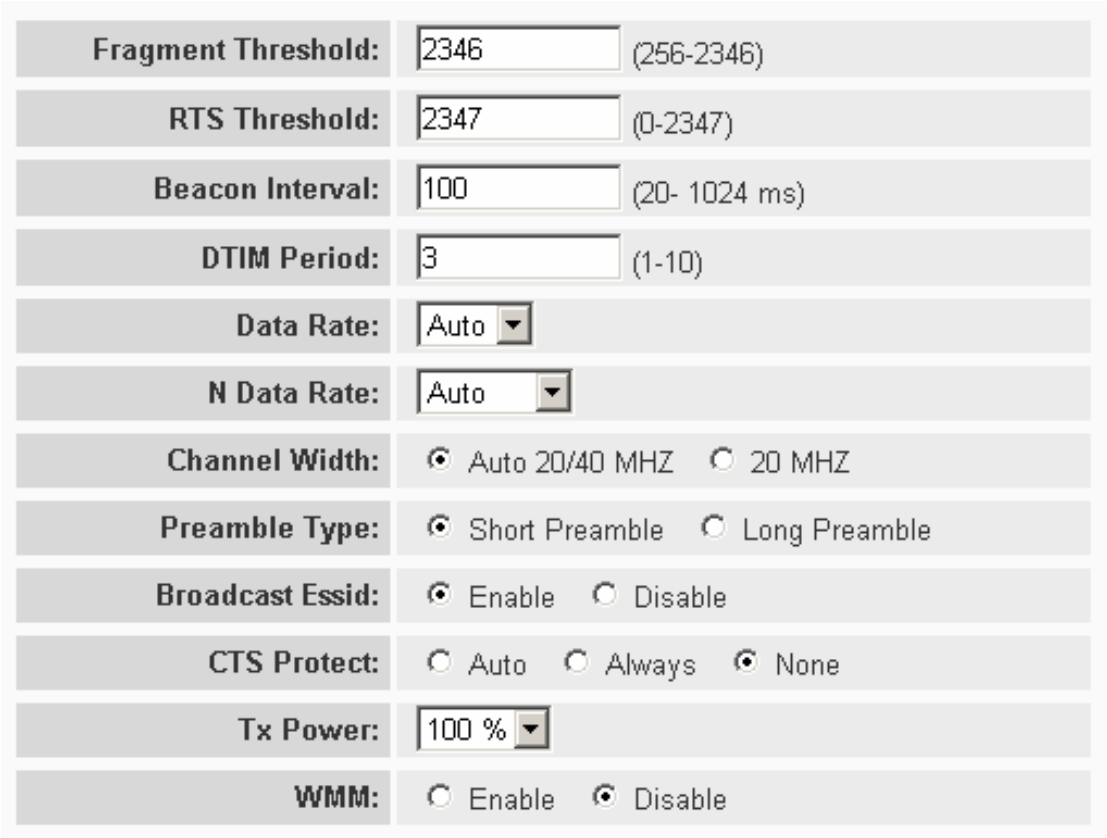


Parameter	Description
Mode	It allows user to set the following mode: AP, Station, Bridge or WDS mode.
Band	It allows user to set the AP to be fixed at 802.11b, 802.11g or 802.11n mode. Users also can select B+G+N mode to allow the router to select among 802.11b, 802.11g and 802.11n connection automatically.
ESSID	This is the name of the wireless LAN. All the devices in the same wireless LAN should have the same ESSID.
Channel Number	The channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel.
MAC address	If users want to bridge more than one network together with wireless LAN, it is necessary to set this access point in the following modes: “AP Bridge-Point to Point mode”, “AP Bridge-Point to Multi-Point mode” or “AP Bridge-WDS mode”. Users have to enter the MAC addresses of other access points that join the bridging work.
Set Security	Click the **<Set Security>** button for “Security Settings” window to pop up. Users can set the security parameters used to bridge access points together when the AP is in AP Bridge modes.

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

4.2.4.2 Advanced Wireless Settings

This router provides some advanced control of wireless parameters. If users want to configure these settings, please click **<Wireless>** menu on the left of web management interface, and then click **<Advanced Settings>**. The following message will be displayed on the web browser.


Fragment Threshold: 2346 (256-2346)
RTS Threshold: 2347 (0-2347)
Beacon Interval: 100 (20- 1024 ms)
DTIM Period: 3 (1-10)
Data Rate: Auto
N Data Rate: Auto
Channel Width: Auto 20/40 MHZ 20 MHZ
Preamble Type: Short Preamble Long Preamble
Broadcast Essid: Enable Disable
CTS Protect: Auto Always None
Tx Power: 100 %
WMM: Enable Disable

Parameter	Description
Fragment Threshold	"Fragment Threshold" specifies the maximum size of packet during the fragmentation of data to be transmitted. If users set this value too low, it will result in bad performance. *Default: 2346.*
RTS Threshold	When the packet size is smaller the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet. *Default: 2347.*
Beacon Interval	The interval of time that this wireless router broadcast a beacon. Beacon is used to synchronize the wireless network. *Default: 100.*

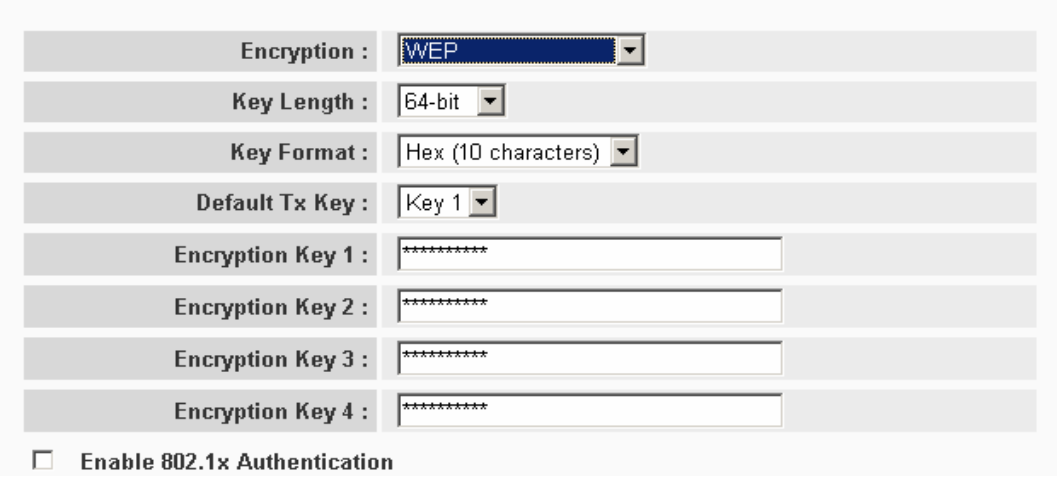
DTIM Period	Set the DTIM period of wireless radio. *Default: 3.*
Data Rate	The “Data Rate” is the rate this access point uses to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets.
N Data Rate	Same parameter as above but for 802.11n clients.
Preamble Type	The “Long Preamble” can provide better wireless LAN compatibility, while the “Short Preamble” can provide better wireless LAN performance.
Broadcast ESSID	If “Broadcast ESSID” is enabled, every wireless station located within the coverage of this access point can discover this access point easily. If users are building a public wireless network, enabling this feature is recommended. Disabling “Broadcast ESSID” can provide better security.
CTS Protect	Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g wireless access points. It’s recommended to set this option to ‘Auto’ or ‘Always’.
Tx Power	Users can set the output power of wireless radio. Unless the user is using this wireless router in a really big space, it is not necessary to set output power to 100%.
Turbo Mode	Enhance the data transfer rate of LAN (up to 35Mbps, only for 11g). *Default: ‘Enabled’.*
WMM	WMM is short for Wi-Fi Multimedia which will enhance the data transfer performance of multimedia contents when transferred over wireless network. *Default: ‘Disabled’.*

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

4.2.4.3 Wireless Security

To set wireless security settings, please click **<Wireless>** menu on the left of web management interface and then click **<Security Settings>**. Follow the following instructions to set wireless security settings.

WEP Only

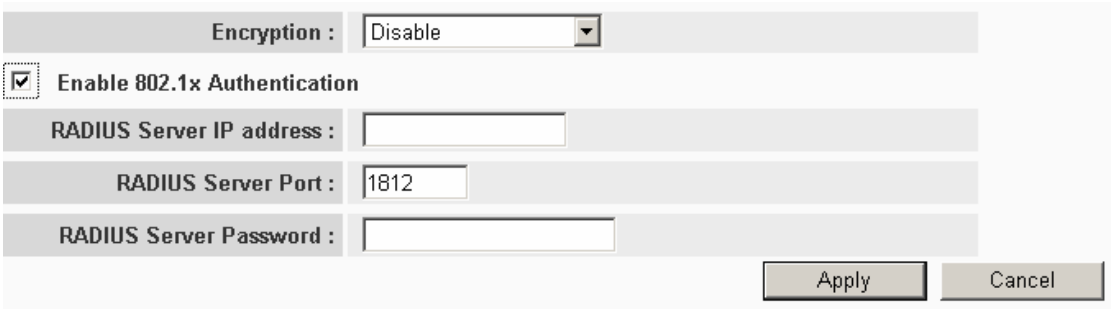

Encryption : WEP
Key Length : 64-bit
Key Format : Hex (10 characters)
Default Tx Key : Key 1
Encryption Key 1 : **********
Encryption Key 2 : **********
Encryption Key 3 : **********
Encryption Key 4 : **********
Enable 802.1x Authentication

Parameter	Description
Key Length	Users can select the WEP key length for encryption, 64-bit or 128-bit. Larger WEP key length will provide higher level of security, but the throughput will be lower. Default: 64-bit
Key Format	There are two types of key format: ASCII and Hex. When users select a key format, the number of characters of key will be displayed. For example, if users select '64-bit' as key length, and 'Hex' as key format, the message at the right of 'Key Format' is 'Hex (10 characters), which means the length of WEP key is 10 characters.
Default Key	Select one of the four keys to encrypt the data. Only the key selected in the "Default key" will take effect.
Key 1 - Key 4	The WEP keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. • 64-bit WEP: input 10-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. • 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 13-digit ASCII characters as the encryption keys.

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

802.1x only

IEEE 802.1x is an authentication protocol and every user must use a valid account to login before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encrypt the data during communication.

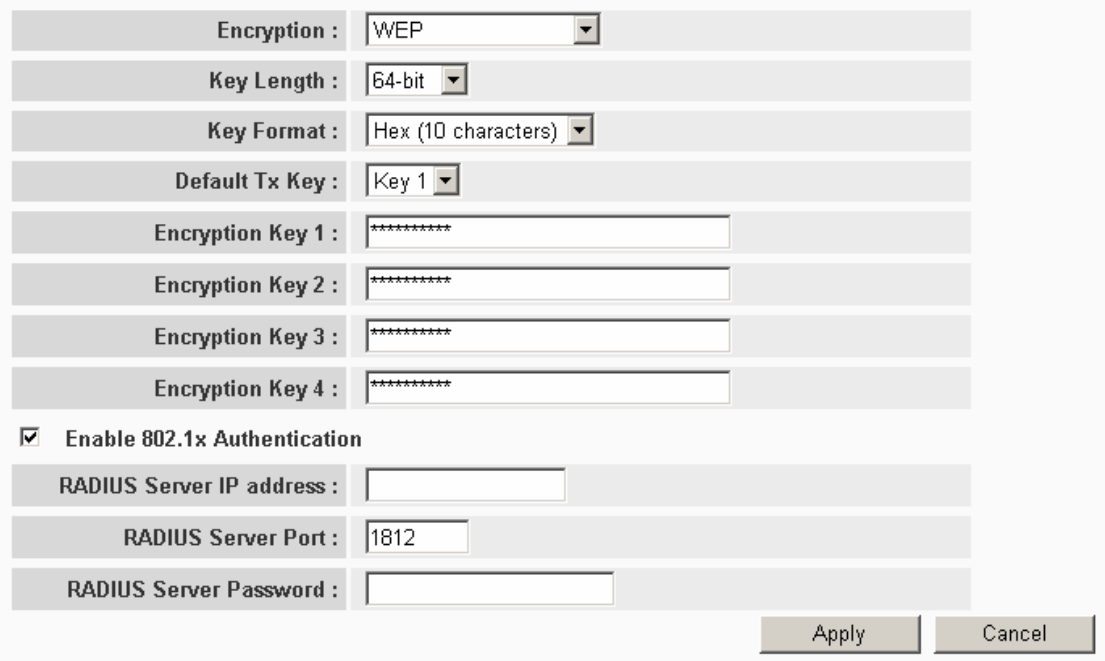


Parameter	Description
RADIUS Server IP address	The IP address of external RADIUS server.
RADIUS Server Port	The service port of the external RADIUS server.
RADIUS Server Password	The password used by external RADIUS server.

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

802.1x WEP Static key

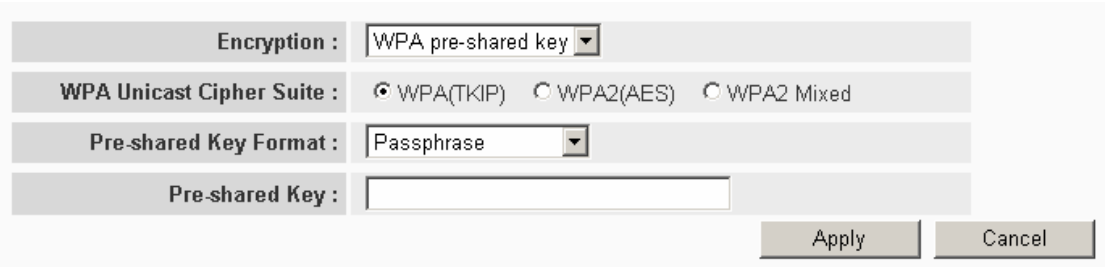
IEEE 802.1x is an authentication protocol and every user must use a valid account to login before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode also uses WEP to encrypt the data during communication.



Refer to relevant sections for WEP and 802.1x configurations.

WPA Pre-shared key

Wi-Fi Protected Access (WPA) is an advanced security standard. Users can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be broken by hackers.



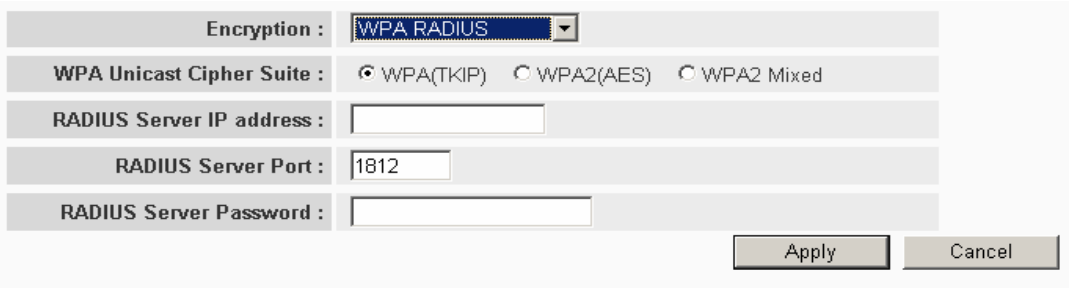
Parameter	Description
WPA(TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
WPA2(AES)	This use CCMP protocol to change encryption key frequently. AES can provide high level encryption to enhance the wireless LAN security.
WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.

Pre-shared Key Format	Users may select to a pass phrase (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the Pre-shared Key. *For example:* *Pass phrase: iamguest* *Hexadecimal Digits: 12345abcde*
Pre-shared Key	The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill in the text box by following the rules below. *Hex WEP: input 64-digit* *Hex values (in the “A-F”, “a-f” and “0-9” range) or at least 8 character pass phrase as the pre-shared keys.*

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

WPA Radius

Wi-Fi Protected Access (WPA) is an advanced security standard. Users can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently.

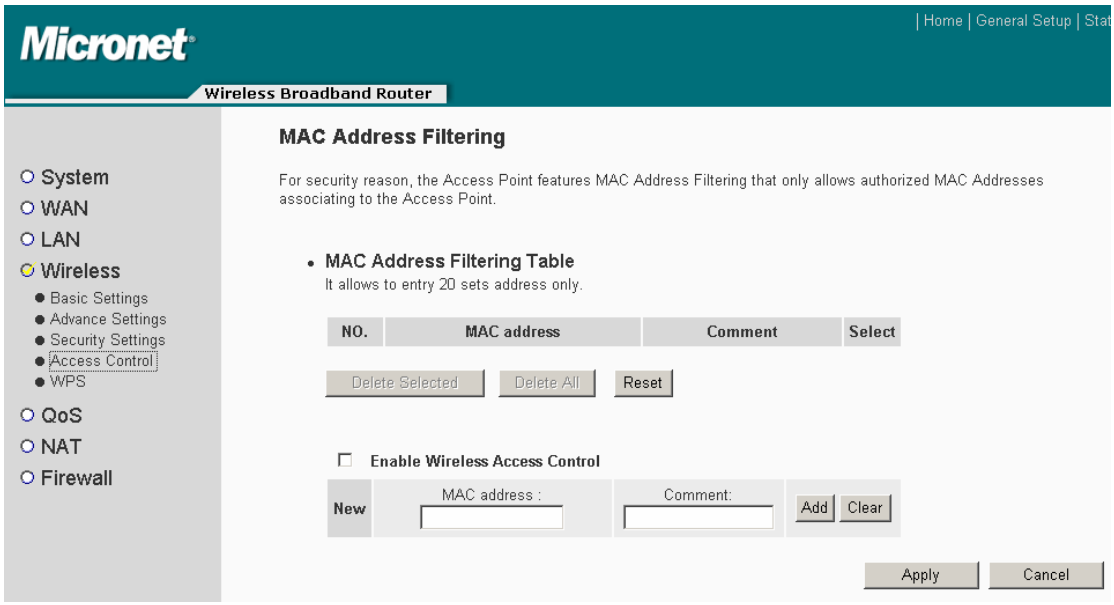


Parameter	Description
WPA(TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
WPA2(AES)	This use CCMP protocol to change encryption key frequently. AES can provide high level encryption to enhance the wireless LAN security.
WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.
RADIUS Server IP address	The IP address of external RADIUS server.
RADIUS Server Port	The service port of the external RADIUS server *Default: 1812.*
RADIUS Server Password	The password used by external RADIUS server.

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

4.2.4.4 Wireless Access Control

This wireless router provides MAC Address Control, which prevents the unauthorized MAC addresses from accessing the wireless network.



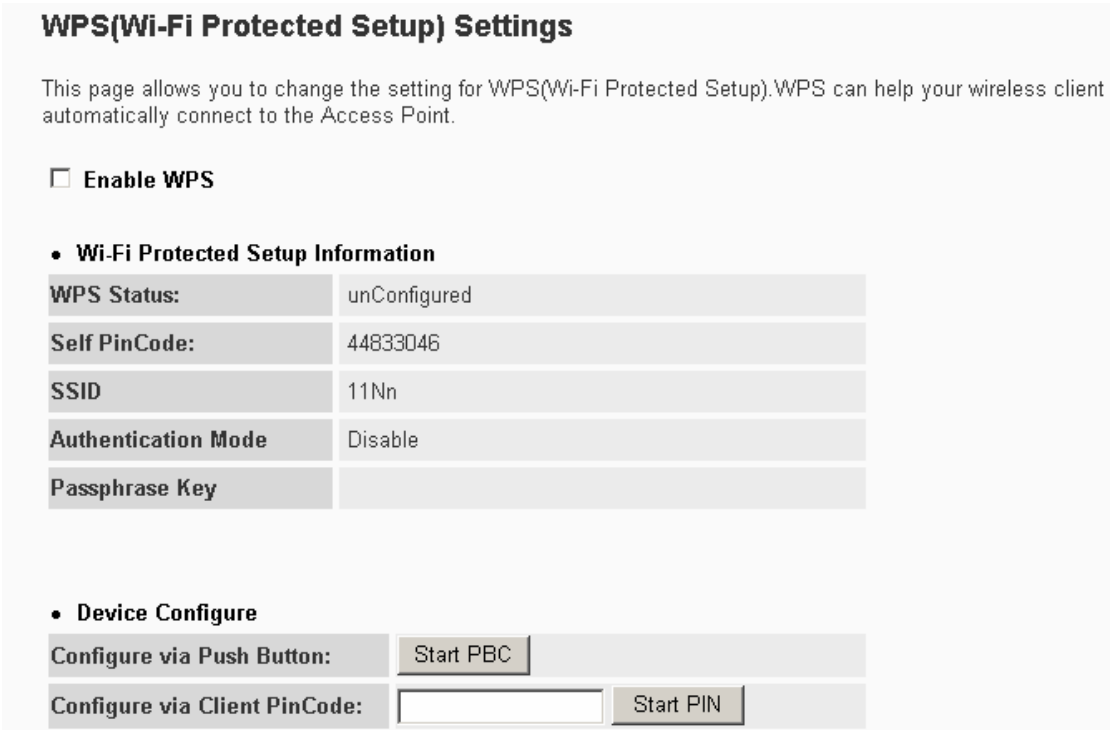
Parameter	Description
Enable wireless access control	Allow enabling of access control for wireless connection.
Add MAC address into the list	Fill in the "MAC Address" and "Comment" of the wireless station to be added. Click **<Add>** to for this wireless station to be added into the "Current Access Control List". Click **<Clear>** for both "MAC Address" and "Comment" fields to be cleared.
Remove MAC address from the list	If users want to remove a MAC address from the "Current Access Control List ", select the MAC addresses to be deleted and click **<Delete Selected>**. Click **<Delete All>** button to remove all MAC addresses. Click **<Reset>** will clear current selections.

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

4.2.4.5 WPS

Wi-Fi Protected Setup (WPS) is the simplest way to build connection between wireless network clients and the wireless router. Users don't have to select encryption mode and input a long encryption passphrase every time setting up a wireless client. This wireless router supports two types of WPS: Push-Button Configuration (PBC) and PIN code. If users want to use PBC, it is necessary to push a specific button on the wireless client to start WPS mode, and switch this wireless router to WPS mode too. You can push Reset/WPS button of this wireless router, or click 'Start PBC' button in the web configuration interface. If users want to use PIN code, it is necessary to know the PIN code of wireless client and switch it to WPS mode, then provide the PIN code of the wireless client to connect to this wireless router. The detailed instructions are listed follow:

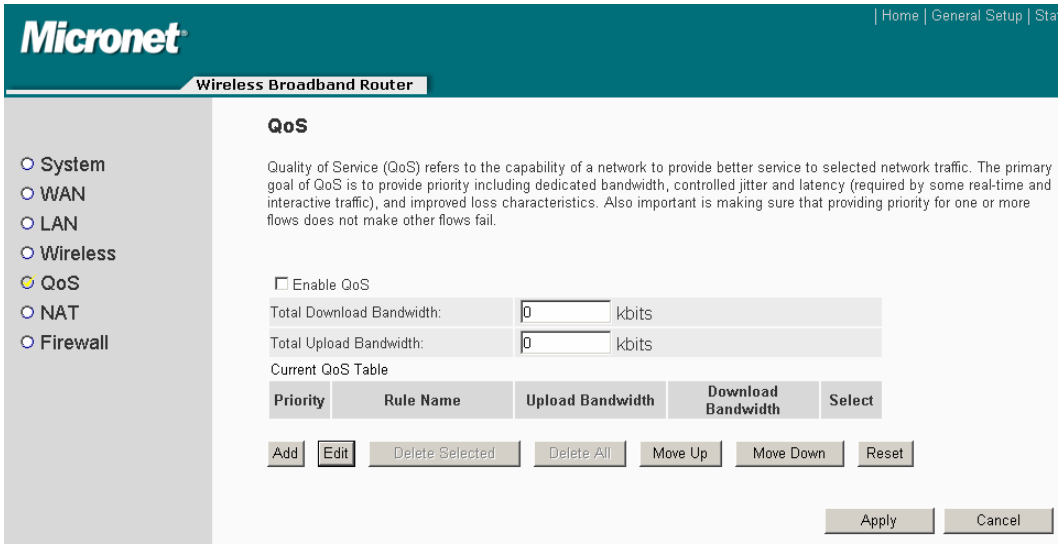
Please click **<Wireless>** menu on the left of web management interface and click **'WPS'**. The following message will be displayed on the web browser.


WPS(Wi-Fi Protected Setup) Settings
This page allows you to change the setting for WPS(Wi-Fi Protected Setup).WPS can help your wireless client automatically connect to the Access Point.
Enable WPS
Wi-Fi Protected Setup Information
WPS Status: unConfigured
Self PinCode: 44833046
SSID 11Nn
Authentication Mode Disable
Passphrase Key
Device Configure
Configure via Push Button: Start PBC
Configure via Client PinCode: Start PIN

Parameter	Description
Enable WPS	Check this box to enable WPS function, uncheck it to disable WPS.
WPS Status	If the wireless security (encryption) function of this wireless router is properly set, users will see 'Configured' message.
Self PIN code	This is the WPS PIN code of this wireless router. This code is useful when users need to build wireless connection by WPS with other WPS-enabled wireless devices.
SSID	The SSID of this wireless router will be displayed here.
Authentication Mode	The wireless security authentication mode of this wireless router will be displayed here.
Configure via Push Button	Click <Start PBC> to start Push-Button style WPS via Push Button setup procedure. This wireless router will wait for WPS requests from wireless clients for 2 minutes. The 'WLAN' LED on the wireless router will be steady on when this wireless router is waiting for incoming WPS request.
Configure via Client Pin Code	Please input the PIN code of the wireless client you wish to connect, and click **<Start PIN>** button. The 'WLAN' led on the wireless router will be steady on when this wireless router is waiting for incoming WPS request.

4.2.5 QoS

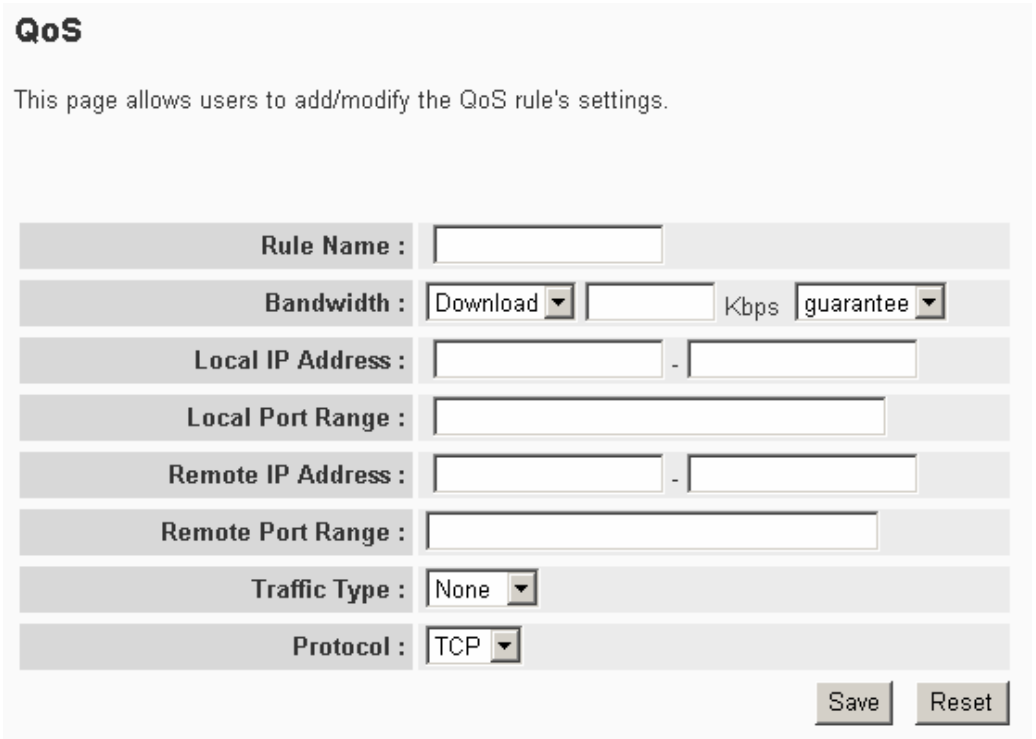
Quality of service provides an efficient way for computers on the network to share the Internet bandwidth with a promised quality of internet service. Without QoS, all computers and devices on the network will compete with each other to get Internet bandwidth, and some applications which require guaranteed bandwidth (like video streaming and network telephone) will be affected. Therefore an unpleasing result will occur, like the interruption of video / audio transfer.


Micronet
Wireless Broadband Router
| Home | General Setup | Sta
System
WAN
LAN
Wireless
QoS
NAT
Firewall
QoS
Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail.
Enable QoS
Total Download Bandwidth: 0 kbits
Total Upload Bandwidth: 0 kbits
Current QoS Table
Priority
Rule Name
Upload Bandwidth
Download Bandwidth
Select
Add
Edit
Delete Selected
Delete All
Move Up
Move Down
Reset
Apply
Cancel

Parameter	Description
Enable/Disable QoS	Allow enable or disable of QoS function.
Add a QoS rule into the table	Click **<Add>** to enter the form page for the QoS rule. Click **<Apply>** after filling out the form and the rule will be added into the table.
Remove QoS rules from the table	If users want to remove a QoS rules from the table, select the QoS rules and click **<Delete Selected>**. To remove all QoS rules from the table, click **<Delete All>** button. Click **<Reset>** will clear the current selections.
Edit a QoS rule	Select the rule to edit and click **<Edit>**, then it will enter the detail form of the QoS rule. Click **<Apply>** after editing the form and the rule will be saved.
Adjust QoS rule priority	Users can select the rule and click **<Move Up>** to make the priority higher. Select the rule and click **<Move Down>** to make the priority lower.

4.2.5.1 Edit QoS Rule

Users can assign packet classification criteria by its local IP range, remote IP range, traffic type, protocol, local port range and remote port range parameters. The parameters that users leave as blank will be ignored. The priority of this rule will be applied to packets that match classification criteria of this rule. It can limit bandwidth consumed by packets that match this rule or guarantee bandwidth required by packets that match this rule.

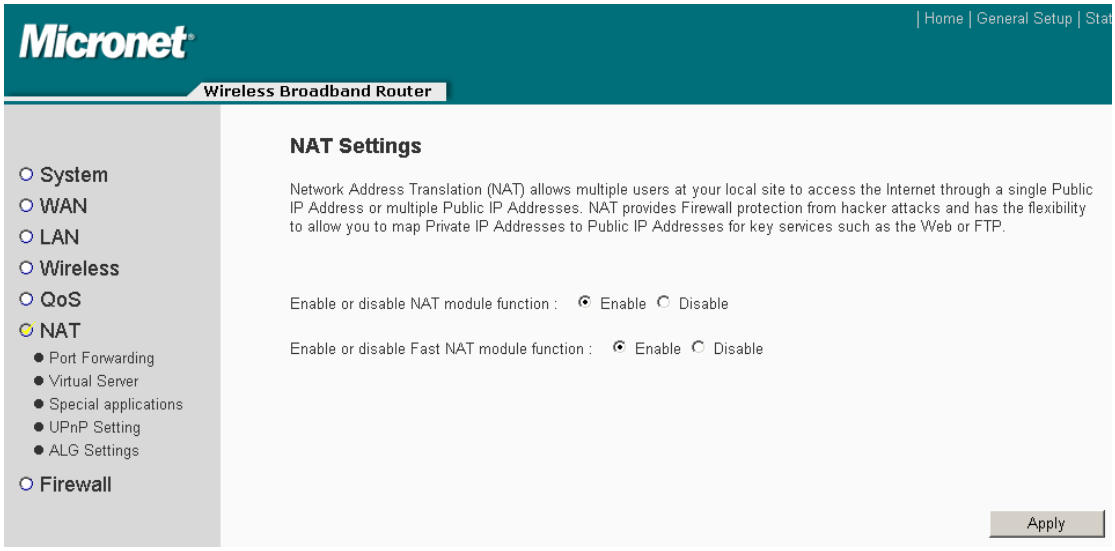


Parameter	Description
Rule Name	The name of this rule.
Bandwidth	Users can assign the download or upload bandwidth in the unit of Kbps (1024 bit per second). It can limit the maximum bandwidth consumed by this rule by selecting “Maximum”. Reserve enough bandwidth for this rule by selecting “Guarantee”.
Local IP Address	Enter the local IP address range of the packets that this rule will apply. If users assign 192.168.2.3 – 192.168.2.5, it would mean 3 IP addresses: 192.168.2.3, 192.168.2.4 and 192.168.2.5.
Local Port Range	Enter the local port range of the packets that this rule will apply. Users can assign a single port number here or assign a range of port numbers by assigning the first port number and the last port number of the range. The two numbers are separated by a dash “-“, for example “100-150” means from port number 100 to port number 150 – the range of 50 port numbers.
Remote IP Address	Enter the remote IP address range of the packets that this rule will apply. If users assign 192.168.2.3 – 192.168.2.5, it means 3 IP addresses: 192.168.2.3, 192.168.2.4 and 192.168.2.5.
Remote Port Range	Enter the remote port range of the packets that this rule will apply. Users can assign a single port number here or assign a range of port numbers by assigning the first port number and the last port number of the range. The two numbers are separated by a dash “-“, for example “101-150” means from port number 100 to port number 150 – the range of 50 port numbers.
Traffic Type	Select the traffic type of the packets that this rule will apply. List of some popular applications is already available for easing the configuration. Users also can get the same result by using other parameters.
Protocol	Select the protocol type of the packets that this rule will apply.
Save	Save and exit the form.
Reset	Clear the content of this form.

*Click **<Save>** at the bottom of the screen to save the above configurations.*

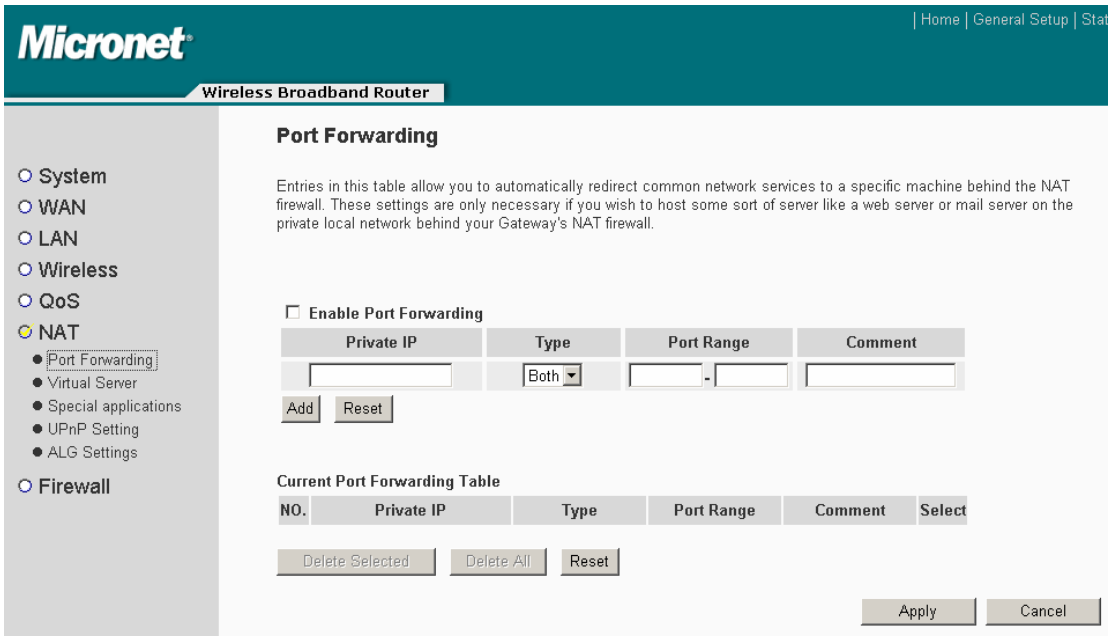
4.2.6 NAT

Network address translations solve the problem of sharing a single IP address to multiple computers. Without NAT, all computers must be assigned with a valid Internet IP address to connect to Internet. Therefore it’s necessary to use NAT technology to share a single Internet IP address to multiple computers on local network, so everyone can connect to Internet.


Micronet
Wireless Broadband Router
| Home | General Setup | Stat
System
WAN
LAN
Wireless
QoS
NAT
Port Forwarding
Virtual Server
Special applications
UPnP Setting
ALG Settings
Firewall
NAT Settings
Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as the Web or FTP.
Enable or disable NAT module function : Enable Disable
Enable or disable Fast NAT module function : Enable Disable
Apply

4.2.6.1 Port Forwarding

This function allows user to redirect a single port or consecutive ports of Internet IP address to the same port of the IP address on local network. The port number(s) of Internet IP address and private IP address (the IP address on local network) must be the same. If the port number of Internet IP address and private IP address is different, please use 'Virtual Server' function, described in next section.

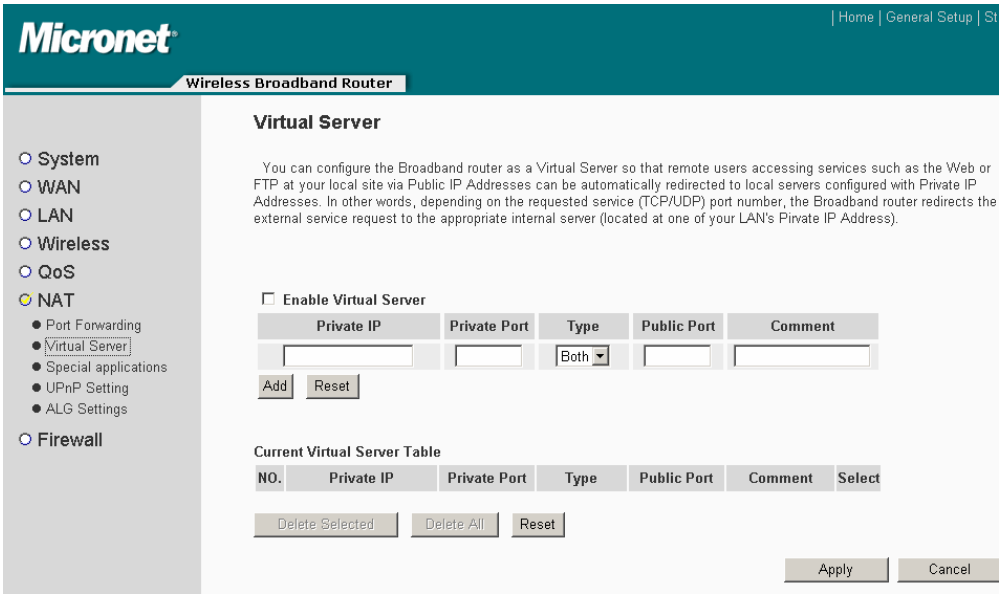


Parameter	Description
Enable Port Forwarding	Allow port forwarding to be enabled.
Private IP	This is the private IP of the server behind the NAT firewall. Users will need to give the LAN PC clients a fixed/static IP address for Port Forwarding to work properly.
Type	This is the protocol type to be forwarded. Users can choose to forward “TCP” or “UDP” packets only or select “both” to forward both “TCP” and “UDP” packets.
Port Range	The range of ports to be forward to the private IP.
Comment	The description of this setting.
Add Port Forwarding into the table	Fill in the "Private IP", “Type”, “Port Range” and "Comment" of the setting and click **<Add>**. This Port Forwarding setting will be added into the "Current Port Forwarding Table". Click **<Reset>** and the fields will be cleared.
Remove Port Forwarding into the table	If users want to remove some Port Forwarding settings from the "Current Port Forwarding Table", select the Port Forwarding setting and click **<Delete Selected>**. Click **<Delete All>** button to remove all settings. Click **<Reset>** to clear the current selection.

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

4.2.6.2 Virtual Server

This function allows user to redirect a port on Internet IP address (on WAN port) to a specified port of an IP address on local network, so it can setup an Internet service on the computer on local network, without exposing it on Internet directly. Users can also build many sets of port redirection to provide many different Internet services on different local computers via a single Internet IP address.

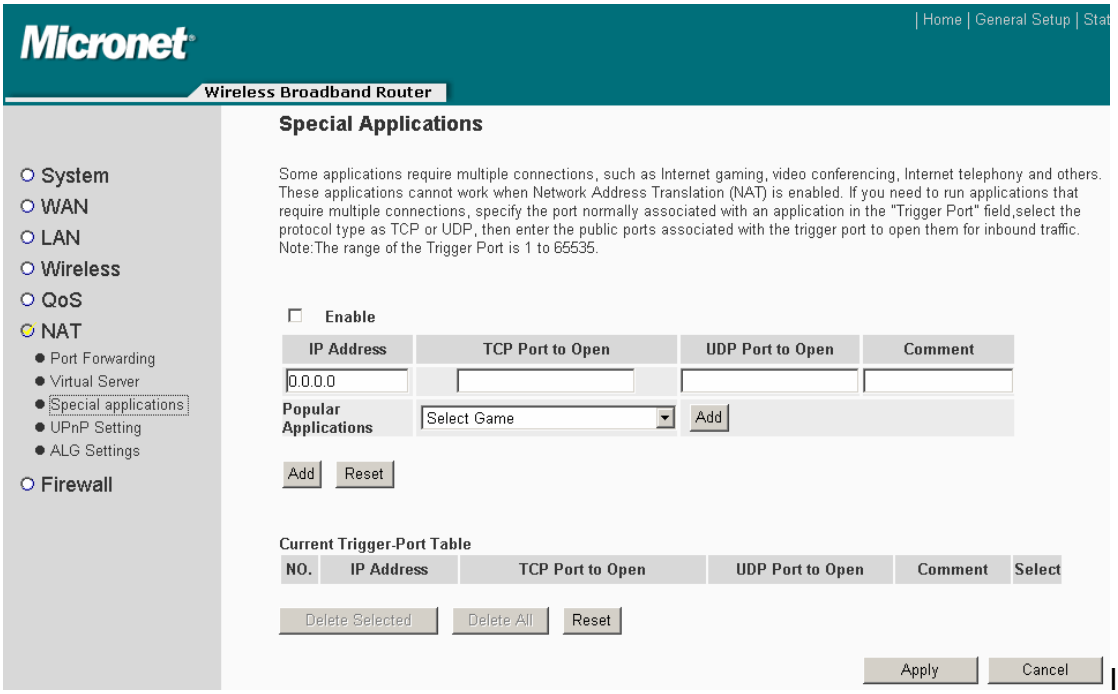


Parameter	Description
Enable Virtual Server	Allow Virtual Server to be enabled.
Private IP	This is the LAN client/host IP address that the Public Port number packet will be sent. Users need to give the LAN PC clients a fixed/static IP address for Virtual Server to work properly.
Private Port	This is the port number (of the above Private IP host) that the below Public Port number will be changed to when the packet enters the LAN (to the LAN Server/Client IP).
Type	Select the port number protocol type (TCP, UDP or both). If users are unsure, then leave it to default.
Public Port	Enter the service (service/Internet application) port number from the Internet that will be redirected to the above Private IP address host in the LAN. Virtual Server function will have priority over the DMZ function if there is a conflict between the Virtual Server and the DMZ settings.
Comment	The description of this setting.
Add Virtual Server	Fill in the "Private IP", "Private Port", "Type", “Public Port” and "Comment" of the setting to be added and click **<Add>**. Then this Virtual Server setting will be added into the "Current Virtual Server Table". Click **<Reset>** and the fields will be cleared.
Remove Virtual Server	If users want to remove some Virtual Server settings from the "Current Virtual Server Table", select the Virtual Server setting and click **<Delete Selected>**. Click **<Delete All>** button to remove all settings. Click **<Reset>** to clear the current selection.

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

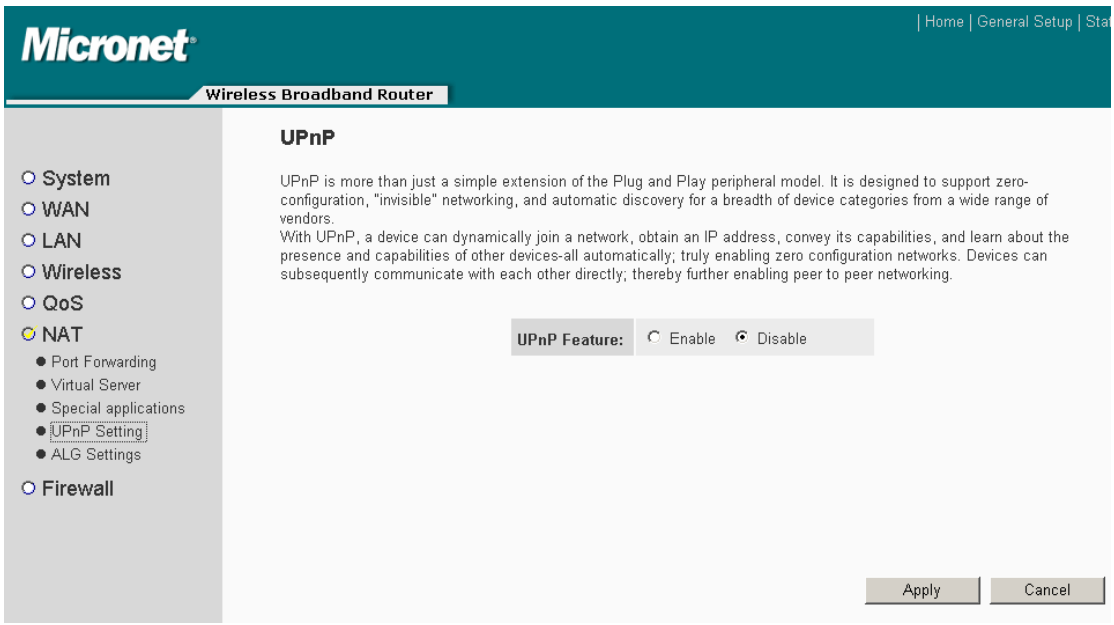
4.2.6.3 Port Mapping for Special Applications

Some applications require more than one connection a time and won’t work with simple NAT rules. In order to make these applications work, users can use this function to let these applications operate properly.



4.2.6.4 UPnP Setting

This function enables network auto-configuration for peer-to-peer communications. Network devices will be able to communicate with other devices directly, and learn information about other devices. Many network device and applications rely on UPnP function nowadays.

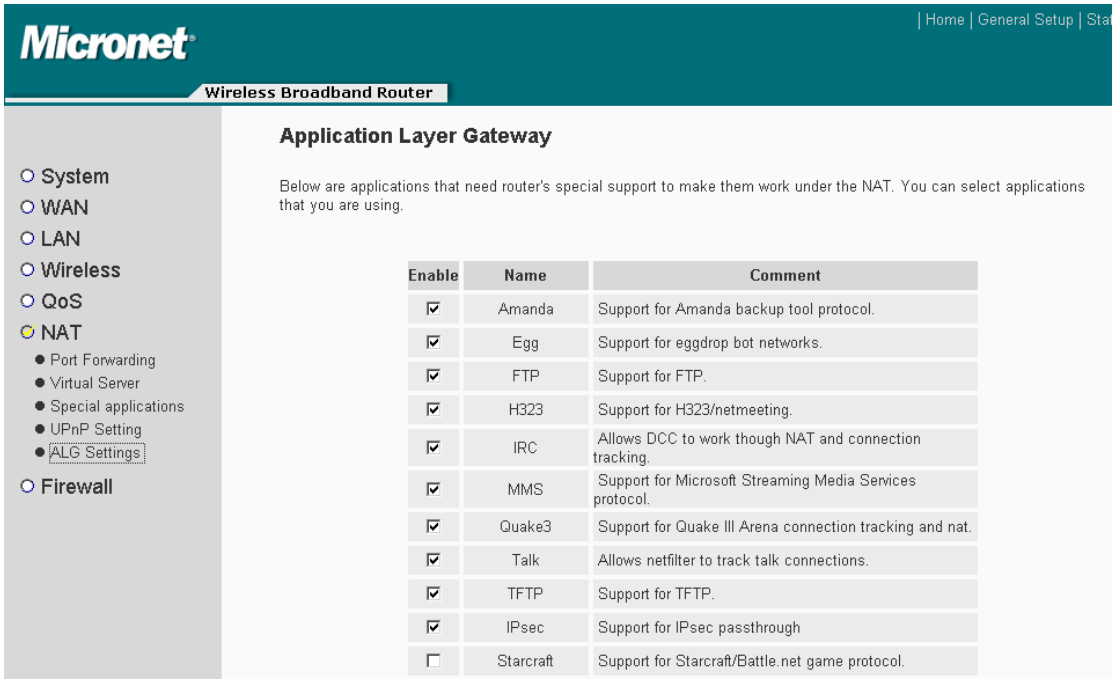

Micronet
Wireless Broadband Router
| Home | General Setup | Stat
System
WAN
LAN
Wireless
QoS
NAT
Port Forwarding
Virtual Server
Special applications
UPnP Setting
ALG Settings
Firewall
UPnP
UPnP is more than just a simple extension of the Plug and Play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors.
With UPnP, a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices-all automatically; truly enabling zero configuration networks. Devices can subsequently communicate with each other directly; thereby further enabling peer to peer networking.
UPnP Feature:
Enable
Disable
Apply
Cancel

Parameter	Description
UPnP Feature	Users can enable or disable the UPnP feature. Enable the UPnP feature, all client systems that support UPnP, like Windows XP, can discover this router automatically and access the Internet through this router without any configuration. The NAT Traversal function provided by UPnP can let applications that support UPnP smoothly connect to Internet sites without any incompatibility problem due to the NAPT port translation.

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

4.2.6.5 ALG Settings

Users can select applications that need “Application Layer Gateway” support.

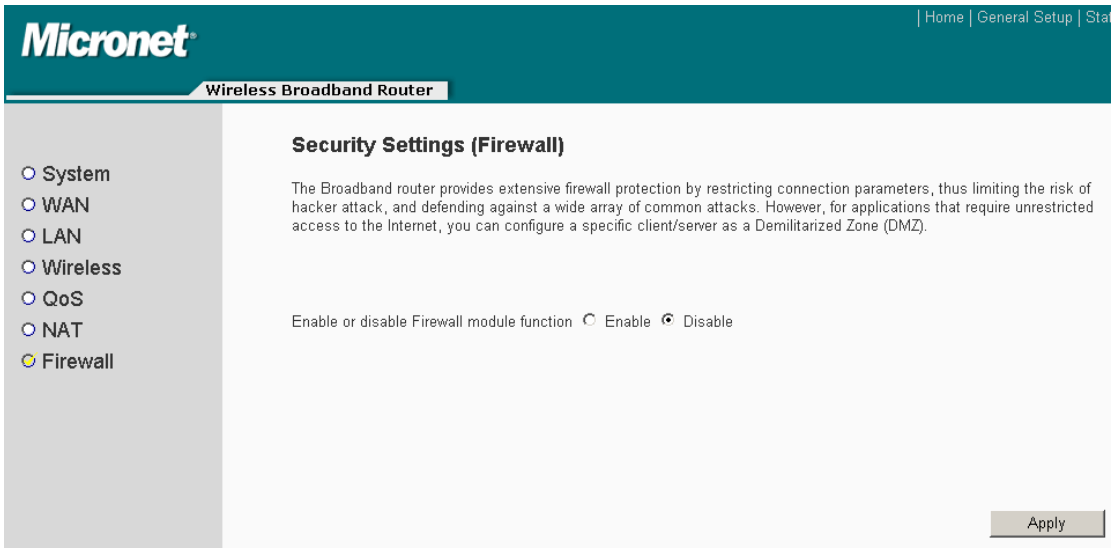


Parameter	Description
Enable	Users can enable “Application Layer Gateway”, and the router will let that application correctly pass though the NAT gateway.

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

4.2.7 Firewall

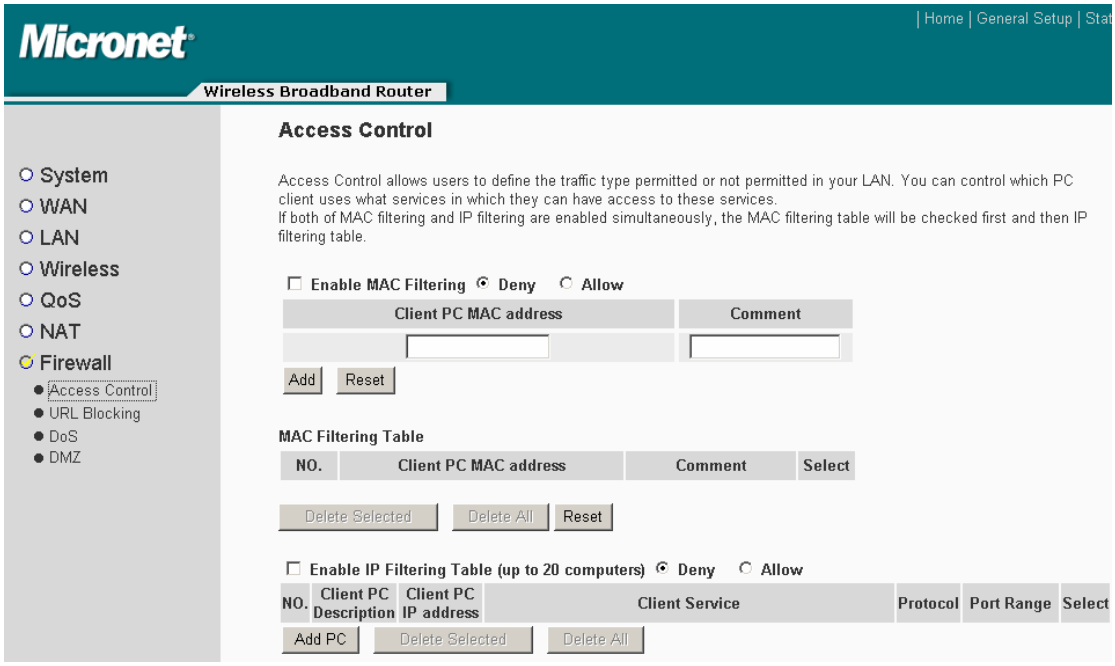
Besides NAT, this router also provides firewall function to block malicious intruders from accessing computers on local network. These functions include inbound attack prevention, and block outbound traffics, like block URLs which have pre-defined keywords.


Micronet
Wireless Broadband Router
| Home | General Setup | Sta
System
WAN
LAN
Wireless
QoS
NAT
Firewall
Security Settings (Firewall)
The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).
Enable or disable Firewall module function Enable Disable
Apply

Parameter	Description
Access Control	Access Control allows user to specify which hosts that the users can or cannot have access to certain Internet applications.
URL Blocking	URL Blocking allows user to specify which URLs cannot be accessed by users.
DoS	The Broadband router's firewall can block common hacker attacks and can log the attack activities.
DMZ	The DMZ function allows user to redirect all packets going to the WAN port IP address to a particular IP address in your LAN.

4.2.7.1 Access Control

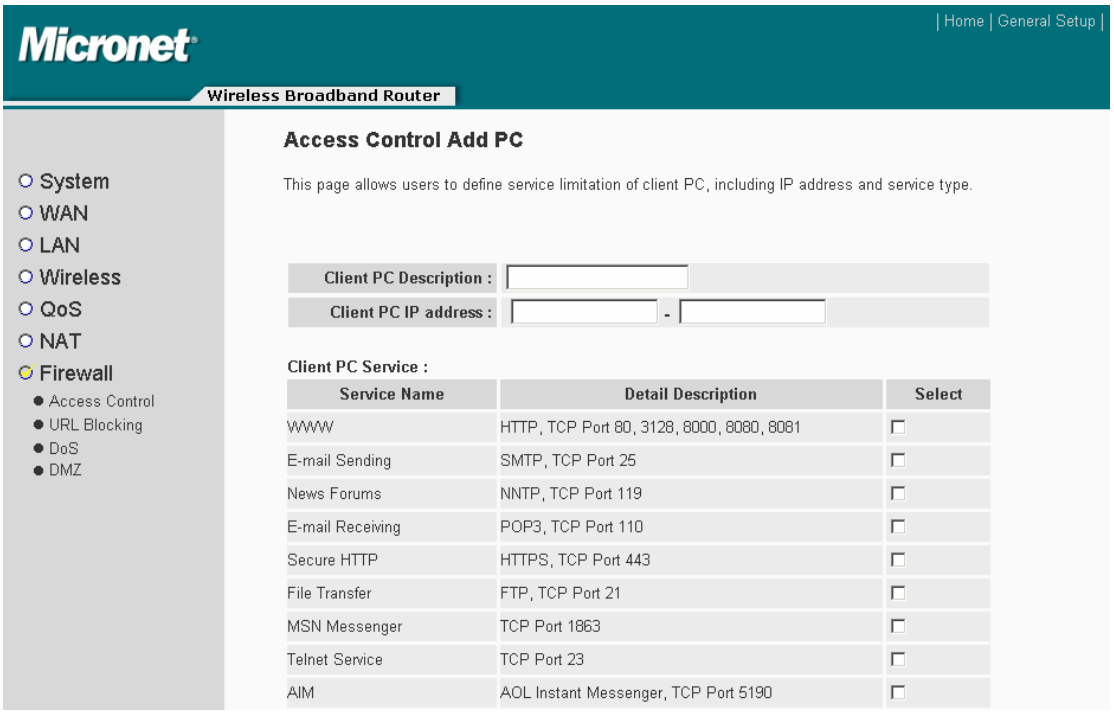
Restrict users from accessing certain Internet applications/services via this interface (e.g. Internet websites, email, FTP etc.). Access Control allows users to define the traffic type permitted in the LAN. Users can control which PC client have access to these services.



Parameter	Description
Deny	If select **<Deny>** then all PCs will be allowed to access Internet besides the PCs in the list below.
Allow	If select **<Allow>** then all PCs will be denied to access Internet except for the PCs in the list below.
Filter client PCs by IP	Fill in “IP Filtering Table” to filter PC clients by IP.
Add PC	Users can click **<Add>** PC to add an access control rule for users by IP addresses.
Remove PC	If users want to remove some PC from the "IP Filtering Table", select the PC and click **<Delete Selected>**. Click **<Delete All>**" button to remove all PCs from the list.
Filter client PC by MAC address	Check **<Enable MAC Filtering>** to enable MAC Filtering.
Add PC	Fill in “Client PC MAC Address” and “Comment” of the PC that is allowed to access the Internet and click **<Add>**. Click **<Reset>** to clear the all fields.
Remove PC	If users want to remove some PC from the "MAC Filtering Table", select the PC and click **<Delete Selected>**. Click **<Delete All>** button to remove all PCs from the table. Click **<Reset>** to clear all selections.

Access Control – Add PC

After button is clicked, the following message will be displayed on the web browser.

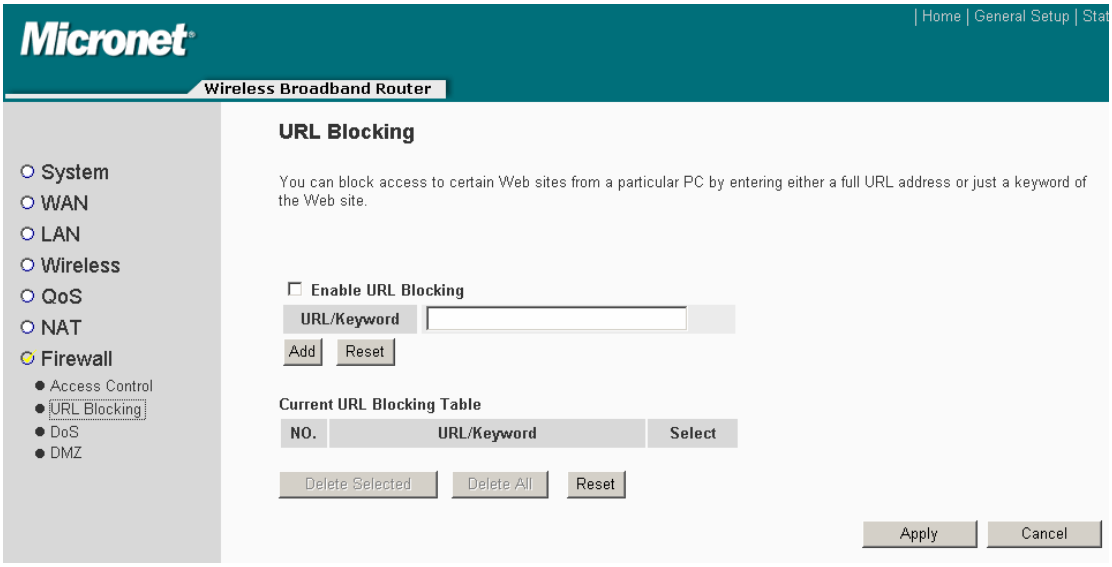


Parameter	Description
Client PC Description	The description for this client PC rule.
Client PC IP Addresses	Enter the IP address range to apply this Access Control rule. Users need to give the LAN PC clients a fixed/static IP address for the Access Control rule to work properly.
Client PC Service	Users can block the clients from accessing some Internet services by checking the services to block.
Protocol	This allows users to select UDP, TCP or both protocol types to block.
Port Range	It can be assign up to five port ranges. The router will block clients from accessing Internet services that use these ports.
Add	Click **<Add>** to save the setting.
Reset	Click **<Reset>** to clear all fields.

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

4.2.7.2 URL Blocking

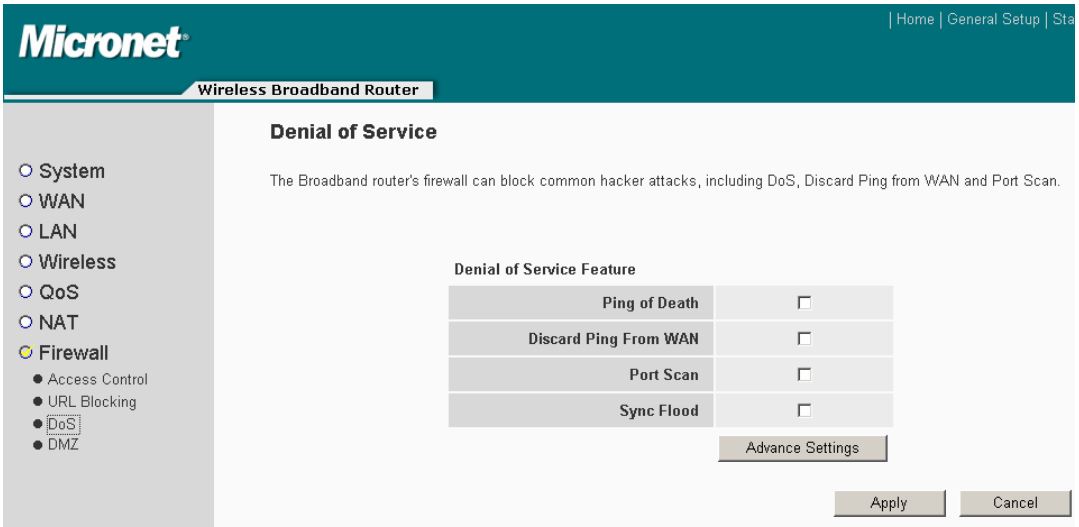
Users can block access to some websites from particular PCs by entering a full URL address or just keyword of the Web site.



Parameter	Description
Enable URL Blocking	Allow URL Blocking to be enabled.
Add URL Keyword	Fill in “URL/Keyword” and then click **<Add>**. Users can enter the full URL address or the keyword of the web site to be blocked. Click **<Reset>** to clear all fields.
Remove URL Keyword	If users want to remove a URL keyword from the "Current URL Blocking Table", select the URL keyword to remove and click **<Delete Selected>**. Click **<Delete All>** button to remove all entries. To clear the selection, just click **<Reset>**.

4.2.7.3 DoS Attack Prevention

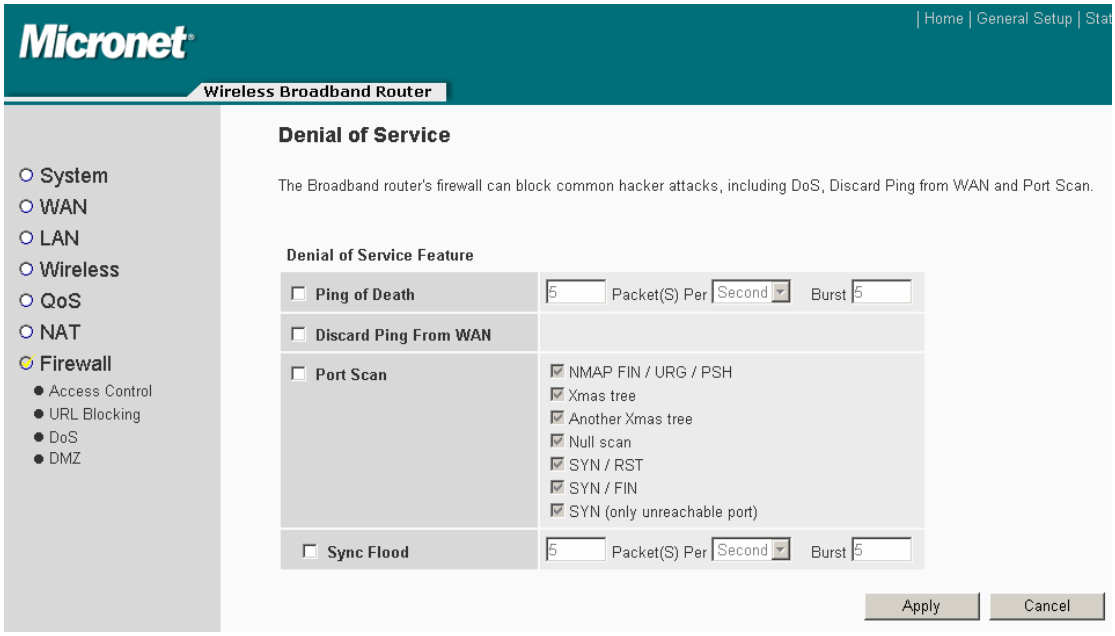
The Broadband router's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. When Internet attacks occur, the router can log the events.



Parameter	Description
Ping of Death	Protections from Ping of Death attack.
Discard Ping From WAN	The router's WAN port will not respond to any Ping requests.
Port Scan	Protect the router from port scan.
Sync Flood	Protect the router from Sync Flood attack.
Advanced Settings	Click on this button to enter the setup of advanced settings for the DoS method.

DoS – Advanced Settings

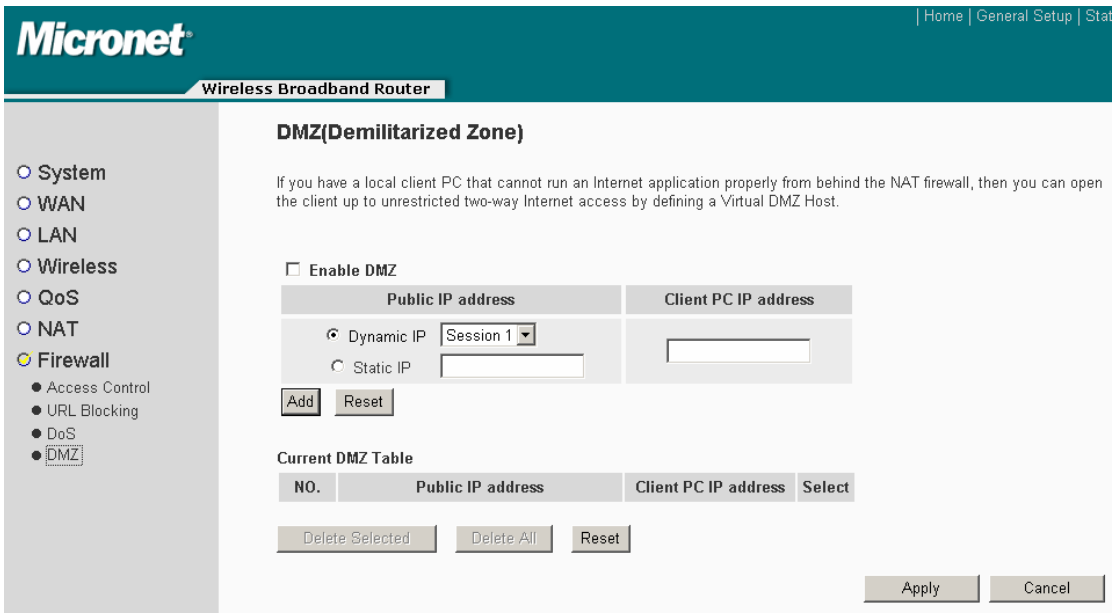
When users click **<Advanced Settings>** button in DoS menu, the following message will be displayed on the web browser.



Parameter	Description
Ping of Death	Set the threshold of when this DoS prevention mechanism will be activated. Please check the box of Ping of Death, and input the frequency of threshold (how many packets per second, minute, or hour). Users can also input the 'Burst' value, which means when this number of 'Ping of Death' packet is received in very short time, this DoS prevention mechanism will be activated.
Discard Ping From WAN	Check the box to activate this DoS prevention mechanism.
Port Scan	Many kind of port scan methods are listed here, please check one or more DoS attack methods to activate.
Sync Flood	Like Ping of Death, users can set the threshold of when this DoS prevention mechanism will be activated.

4.2.7.4 Demilitarized Zone (DMZ)

If users have a local client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, the router can open the client to an unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows re-direct of all packets going to the WAN port IP address to a particular IP address in the LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.



Parameter	Description
Enable DMZ	Allow the DMZ to be enabled. If there is a conflict between the Virtual Server and the DMZ setting, then Virtual Server function will have priority over the DMZ function.
Public IP Address	The IP address of the WAN port or any other Public IP addresses given by the user's ISP.
Client PC IP Address	Input the IP address of a particular host in the LAN that will receive all the packets originally going to the WAN port/Public IP address above. Users need to give the LAN PC clients a fixed/static IP address for DMZ to work properly.

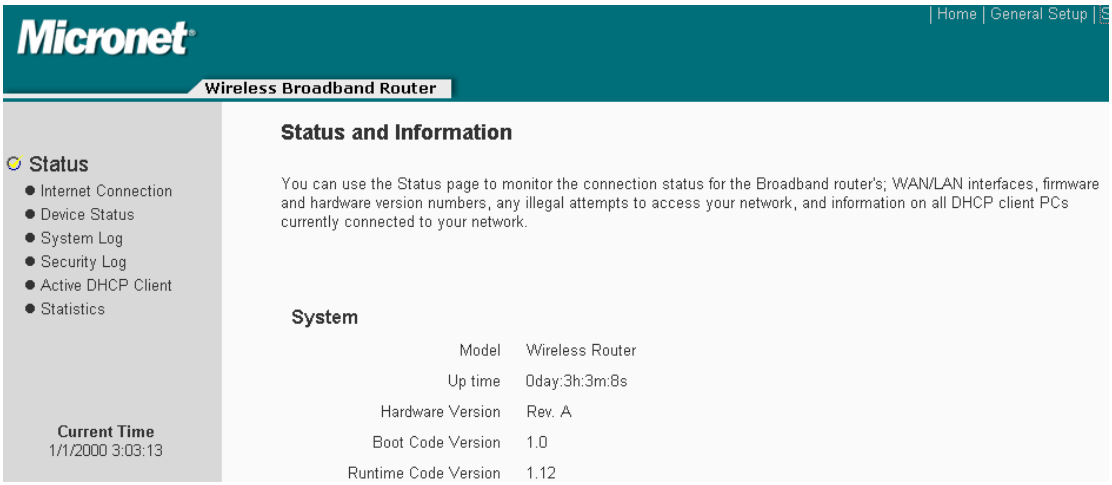
4.3 Status

The Status section allows user to monitor the current status of the router. Use the Status page to monitor following information:

- The connection status of the broadband router WAN/LAN interfaces.
- The current firmware and hardware version numbers.
- Any illegal attempts to access the network, and information on all DHCP client PCs currently connected to the network.

4.3.1 System Information

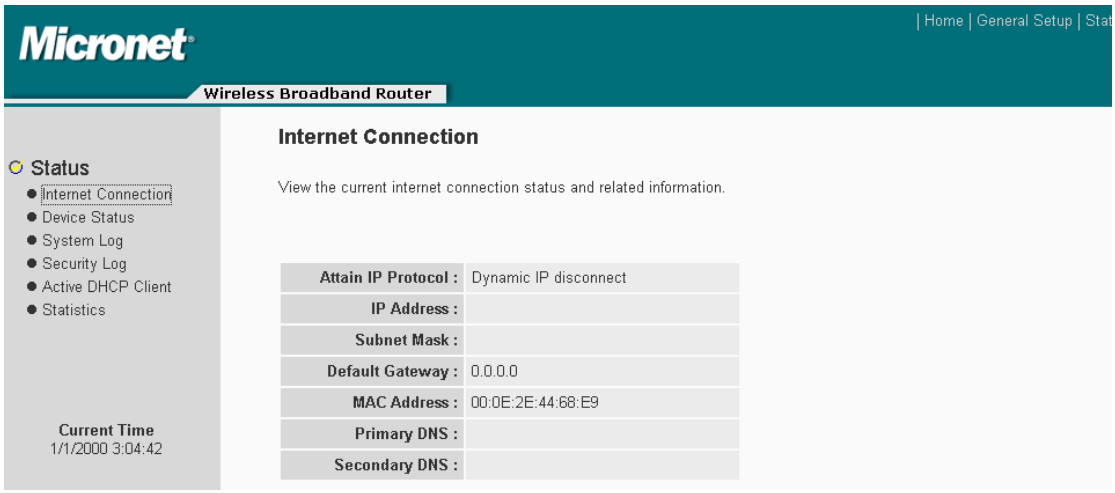
The Status and Information section allows user to view the router's system information.


Micronet
Wireless Broadband Router
| Home | General Setup |
Status
Internet Connection
Device Status
System Log
Security Log
Active DHCP Client
Statistics
Current Time
1/1/2000 3:03:13
Status and Information
You can use the Status page to monitor the connection status for the Broadband router's; WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, and information on all DHCP client PCs currently connected to your network.
System
Model Wireless Router
Up time 0day:3h:3m:8s
Hardware Version Rev. A
Boot Code Version 1.0
Runtime Code Version 1.12

Parameter	Description
Information	Users can view the router's system information such as the router's Hardware version, Serial Number, Boot code Version and Runtime code Version.

4.3.2 Internet Connection Status

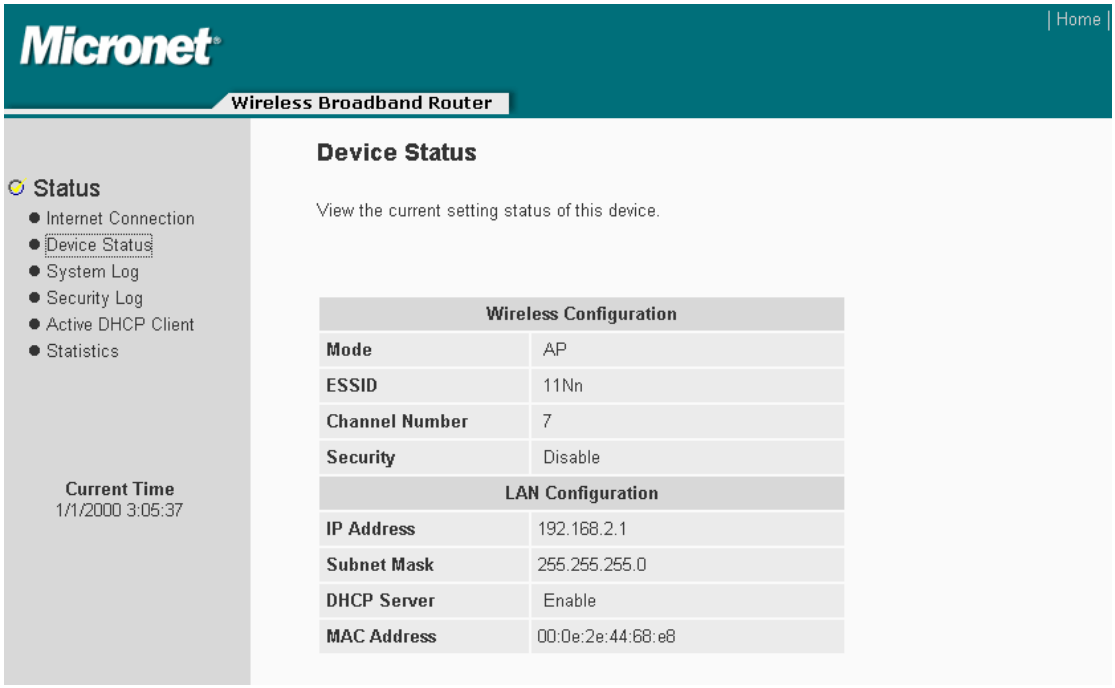
View the broadband router's current Internet connection status and other related information.



Parameter	Description
Internet Connection	This page displays whether the WAN port is connected to a Cable/DSL connection. It also displays the router's WAN port: WAN IP address, Subnet Mask, and ISP Gateway as well as the Primary DNS and Secondary DNS being used.

4.3.3 Device Status

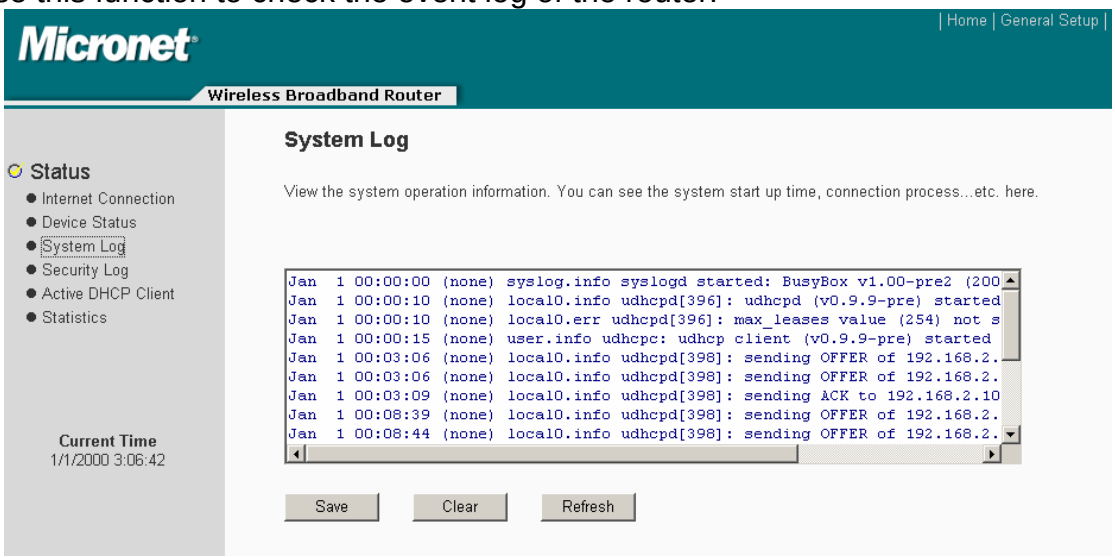
View the broadband router's current configuration settings. The Device Status displays the configuration settings where users have configured in the Quick Setup Wizard/General Setup section.



Parameter	Description
Device Status	This page shows the broadband router's current device settings. This page displays the Broadband router LAN port's current LAN IP Address and Subnet Mask. It also shows whether the DHCP Server function has being enabled or disabled.

4.3.4 System Log

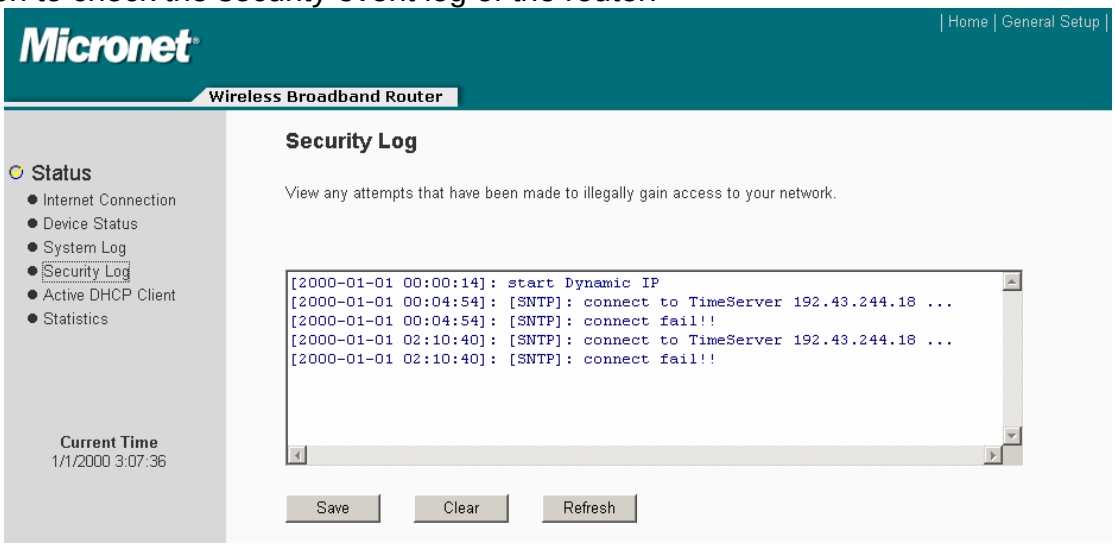
View the operation log of the system. All important system events are logged and users can use this function to check the event log of the router.


Micronet
Wireless Broadband Router
| Home | General Setup |
Status
Internet Connection
Device Status
System Log
Security Log
Active DHCP Client
Statistics
Current Time
1/1/2000 3:06:42
System Log
View the system operation information. You can see the system start up time, connection process...etc. here.
Jan 1 00:00:00 (none) syslog.info syslogd started: BusyBox v1.00-pre2 (200
Jan 1 00:00:10 (none) local0.info udhcpd[396]: udhcpd (v0.9.9-pre) started
Jan 1 00:00:10 (none) local0.err udhcpd[396]: max_leases value (254) not s
Jan 1 00:00:15 (none) user.info udhcpc: udhcp client (v0.9.9-pre) started
Jan 1 00:03:06 (none) local0.info udhcpd[398]: sending OFFER of 192.168.2.
Jan 1 00:03:06 (none) local0.info udhcpd[398]: sending OFFER of 192.168.2.
Jan 1 00:03:09 (none) local0.info udhcpd[398]: sending ACK to 192.168.2.10
Jan 1 00:08:39 (none) local0.info udhcpd[398]: sending OFFER of 192.168.2.
Jan 1 00:08:44 (none) local0.info udhcpd[398]: sending OFFER of 192.168.2.
Save
Clear
Refresh

Parameter	Description
System Log	This page shows the current system log of the broadband router. It displays any event occurred after system start up. At the bottom of the page, the system log can be saved via **<Save>** button to a local file for further processing. The system log can be cleared by clicking **<Clear>** button. Refresh the interface to update current situation, click on **<Refresh>** button. When the system is powered down, the system log will disappear if not saved to a local file.

4.3.5 Security Log

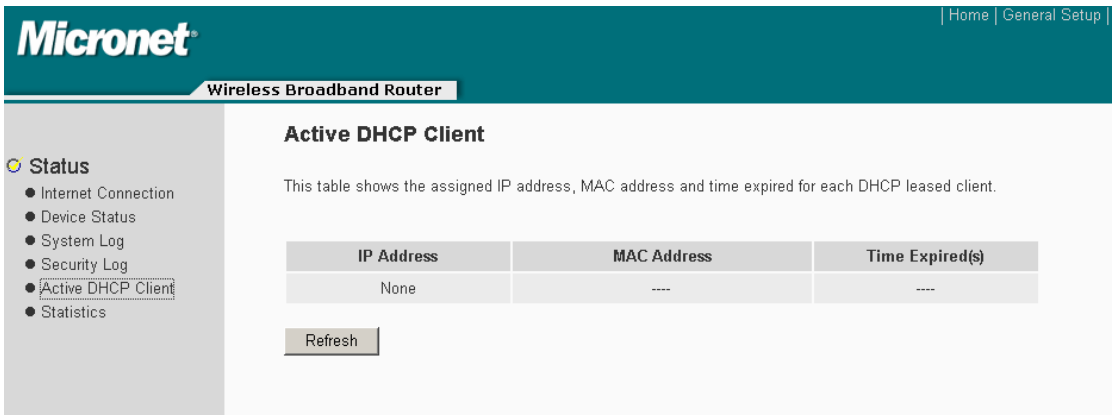
View any attempts that have been made to illegally gain access to the network. All information about network and system security is kept here, and users can use this function to check the security event log of the router.



Parameter	Description
Security Log	This page shows the current security log of the broadband router. It displays any illegal attempts to access the network. At the bottom of the page, the security log can be saved via **<Save>** button to a local file for further processing. The security log can be cleared by clicking **<Clear>** button. Refresh the interface to update current situation, click on **<Refresh>** button. When the system is powered down, the security log will disappear if not saved to a local file.

4.3.6 Active DHCP Client

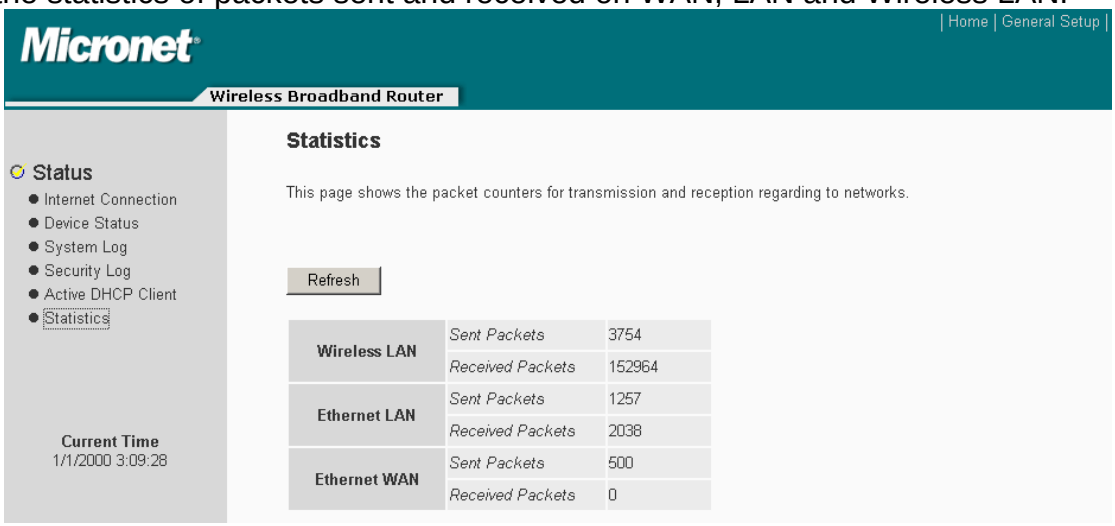
View the LAN client's information that is currently linked to the broadband router's DHCP server.



Parameter	Description
Active DHCP Client	This page shows all DHCP clients (LAN PCs) currently connected to the network. The “Active DHCP Client Table” displays the IP address, the MAC address and Time Expired of each LAN Client. Use the **<Refresh>** button to get the most updated situation

4.3.7 Statistics

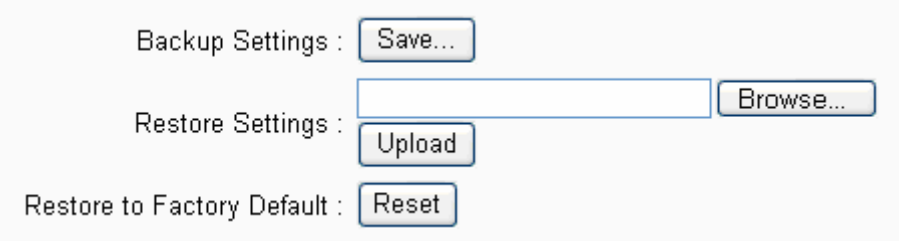
View the statistics of packets sent and received on WAN, LAN and Wireless LAN.



Parameter	Description
Statistics	Shows the counters of packets sent and received on WAN, LAN and Wireless LAN.

4.4 Configuration Backup and Restore

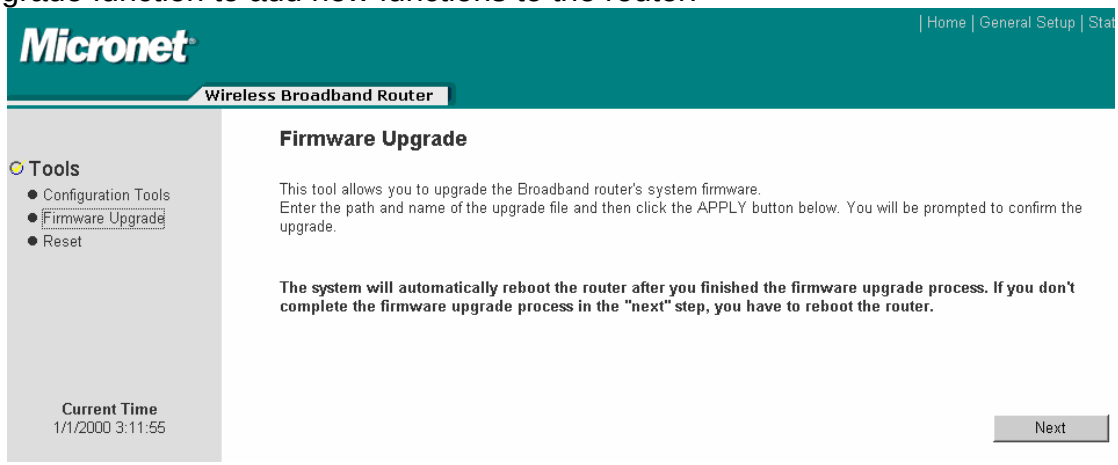
This page includes the basic configuration tools, such as Configuration Tools (save or restore configuration settings), Firmware Upgrade (upgrade system firmware) and Reset.



Parameter	Description
Configuration Tools	Use the "Backup" tool to save the Broadband router current configuration to a file named "config.bin" on the PC. Users can use the "Restore" tool to restore the saved configuration to the broadband router. Alternatively, users can use the "Restore to Factory Defaults" tool to force the Broadband router to perform a power reset and restore the original factory settings.

4.5 Firmware Upgrade

The system software used by this router is called as ‘firmware’. Just like any applications on the computer, when users replace the old application with a new one, the computer will be equipped with new function. Users can also use this firmware upgrade function to add new functions to the router.


Micronet
Wireless Broadband Router
| Home | General Setup | Stat
Tools
Configuration Tools
Firmware Upgrade
Reset
Current Time
1/1/2000 3:11:55
Firmware Upgrade
This tool allows you to upgrade the Broadband router's system firmware.
Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.
The system will automatically reboot the router after you finished the firmware upgrade process. If you don't complete the firmware upgrade process in the "next" step, you have to reboot the router.
Next

Parameter	Description
Firmware Upgrade	This tool allows user to upgrade the broadband router’s system firmware. To upgrade the firmware of the broadband router, users need to download the firmware file to the local hard disk. Enter that file name and path in the appropriate field on this page. Alternatively, use the **<Browse>** button to find the firmware file.

*Click **<Apply>** at the bottom of the screen to save the above configurations.*

4.6 System Reset

Users can reset the router's system should any problem exist. The reset function essentially re-boots the router's system.

Micronet
Wireless Broadband Router
| Home | General Setup | Sta
Tools
Configuration Tools
Firmware Upgrade
Reset
Current Time
1/1/2000 3:12:19
Reset
In the event that the system stops responding correctly or stops functioning,you can perform a Reset. Your settings will not be changed. To perform the reset,click on the APPLY button below. You will be asked to confirm your decision.The Reset will be complete when the LED Power light stops blinking.
Apply
Cancel

Parameter	Description
Reset	In the event that the system stops responding correctly or in some way stops functioning, users can perform a reset. The settings will not be changed. To perform the reset, click on the **<Apply>** button. Users will be asked to confirm your decision. The reset will be complete when the power light stops blinking. Once the reset process is complete users may start using the router again.

Chapter 5 Glossary

Default Gateway (Router): Every non-router IP device needs to configure a default gateway's IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out towards the destination.

DHCP: Dynamic Host Configuration Protocol. This protocol automatically gives every computer on the home network an IP address.

DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as www.Broadbandrouter.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested, the user is sent to the proper IP address. The DNS server IP address used by the computers on the home network is the location of the DNS server assigned by the ISP.

DSL Modem: DSL stands for Digital Subscriber Line. A DSL modem uses the existing phone lines to transmit data at high speeds.

Ethernet: A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

Idle Timeout: Idle Timeout is designed so that when there is no traffic to the Internet for a pre-configured amount of time, the connection will automatically be disconnected.

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods that identifies a single, unique Internet computer host in an IP network. Example: 192.168.2.1. It consists of 2 portions: the IP network address, and the host identifier.

ISP Gateway Address: (see ISP for definition). The ISP Gateway Address is an IP address for the Internet router located at the ISP's office.

ISP: Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN: Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). The home network is considered a LAN.

MAC Address: MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: 3 bytes of data that corresponds to the Manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product's serial number.

NAT: Network Address Translation. This process allows all of the computers on the home network to use one IP address. Using the broadband router's NAT capability, users can access the Internet from any computer on the home network without having to purchase more IP addresses from the ISP.

Port: Network Clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

PPPoE: Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a secure data transmission method originally created for dial-up connections and PPPoE is for Ethernet connections. PPPoE relies on two widely accepted standards, Ethernet and the Point-to-Point Protocol. It is a communications protocol for transmitting information over Ethernet between different manufacturers.

Router: A router is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by the ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocol. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. Both run on top of the IP (Internet Protocol), a network layer protocol.

WAN: Wide Area Network. A network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

Web-based management Graphical User Interface (GUI): Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to Control/configure or monitor the device being managed.